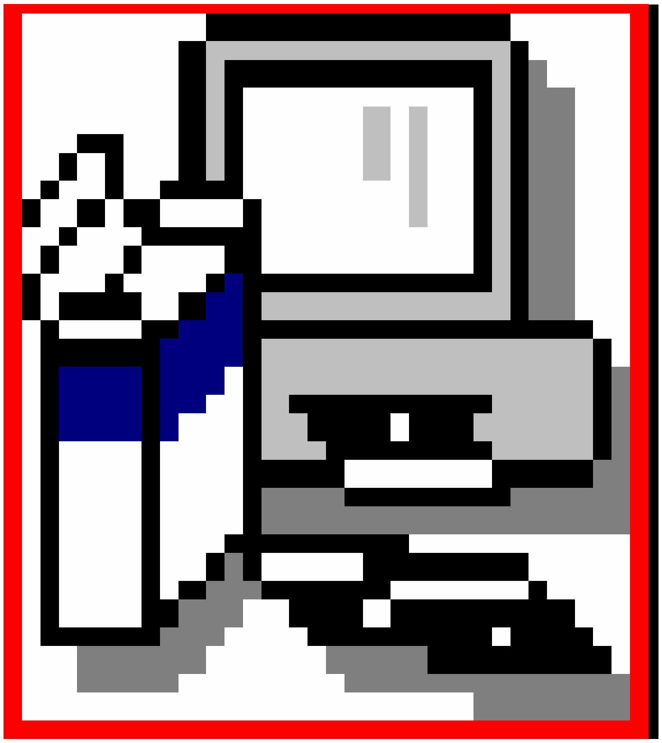
Chapter

7

System Administration

Arizona AIM System



Local Agency User Manual
April 27, 2007

Table of Contents

Chapter 7 - Systems Administration

Capabilities

Purpose

The System Administration functional area is intended to contribute to the overall flexibility, efficiency, and security required for operating and maintaining the AIM System. The functions included in this area are not necessarily WIC Program requirements; they are standard features of a well-designed automated system. This functional area provides the capabilities to maintain information contained in system data (reference) tables, to control general access to the system as well as the ability to perform specific functions, and to move certain files to off-line storage for increased system efficiency.

Security

Administer System Security

Federal regulations require that access to WIC information be restricted to authorized individuals. Access to sensitive health and income information must be limited to those individuals at State and Local agencies that require such information to service WIC participants. The issuance of food instruments is another sensitive area that requires tighter controls than most other management information or participant processing functions. The various controls placed on access to the system as a whole as well as these specific areas constitute a large part of system security.

Administering system security is important because it protects the access to information in the WIC System. System security prevents unauthorized individuals from entering or updating WIC information. It also provides a means of ensuring that only those individuals that have been adequately trained in system operations can access any of the system's functions. Finally, accurate identification of the Users enables the system to create a complete audit trail of all transactions in the system.

In general, the WIC System supports standard security features such as passwords, timed logouts, and terminal lockup after a given number of unsuccessful system access attempts. The system can distinguish between those capabilities that can be performed by a State Agency User and those that can be performed by a Local Agency User. For example, enrollment processing is usually performed at the local level, while vendor management is primarily the domain of the State Agency. In this specific function, the WIC System will allow authorized Users at the State Agency level to add, delete, or update User access and identification information in the system.

The system provides the ability to record and control the specific capabilities of each User at a level defined by the State Agency. State and Local agencies also have the capability to record and review attempts at unauthorized access to the WIC System.

Maintain User Identification and Capabilities

The WIC System allows authorized Users (usually the Local Agency Directors or State Agency Managers) to add, delete, or update Users in the system. When a new User is entered, the system assigns (or accepts from entry) a User Identification that uniquely identifies the User, associates the User with a specific State or Local Agency, and assigns the User an initial password. All Users accessing the WIC application are required to enter their unique ID.

The WIC System controls access to specific functions within the system. Access to these functions is controlled by a series of roles for each User ID in the system that specify which functions the User is authorized to perform. For example, a clerk may be allowed to enter enrollment data, but not allowed to issue a food instrument. The system allows the State-level system administrator to create and modify the roles that will be used.

The System enables authorized Users (e.g., the Local Agency Director) at the Agency level to update these role assignments for each User at their specific site. The system provides a display window that identifies the authorized capabilities and prints a listing with the names of all Users at a site authorized to perform a specific function. Additionally, Local Agency administrators (group administrators) can perform some limited security functions associated with operating a server-based LAN.

The system maintains its security by recording and storing data on authorized Users, limiting User access to functions appropriate for that User category, and monitoring unauthorized access to the system. Additionally, the system restricts User access to data only through the application or appropriate ORACLE tools by function.

The local site system described is a menu driven set of applications requiring several tiers of User access and security. It is assumed that the State Quality Assurance Staff will be responsible for establishing categories of access (guided by State policy), User identification numbers and initial passwords for the various application levels and logon/off procedures.

The system uses unique IDs to identify Users with access to the system. The first security layer occurs when a User boots his or her PC and attempts to sign onto the local network. If this logon is successful, the User's PC displays the Windows Desktop with the AIM System icon. To gain access to the application, the User double clicks on the icon and is presented with another logon window, which actually sits in front of the application. The User is given three (3) attempts to successfully logon to the application. If he or she is unsuccessful, a record of unauthorized access will be captured in the system and the User will be brought back to Windows. If the User is successful, he or she will be brought into the application. To provide this logon/security capability, the system administrator can maintain system security by recording and storing data on authorized Users.

Local Agency system administrators are responsible for adding new Users utilizing network security and the security functionality within the application. The function to maintain internal security tables is only provided to the Local Agency administrator role.

All passwords stored in the application security or utilized in accessing the system are encrypted.

The network operating system provides the capability to make Users change their passwords by periods of time since last password change or on specific dates. This capability can be turned on by the State Systems Administrator at any time and limits the assignment, maintenance and cancellation of operating system passwords to State/Local Administrators.

Monitor Unauthorized Access

The AIM System monitors attempts by Users (who have general access to the system) to gain access to specific functions for which they are not authorized according to the capability list described in the previous capability. The system produces a report, upon request, that lists individuals who have attempted to gain unauthorized access to WIC Functions.

The System detects and tracks three different kinds of access:

- Normal access
- Unauthorized access which failed
- Unusual, successful access

All of these accesses are tracked using the network operating system, ORACLE or application level security. The system has this capability at both the Local Agency and State Agency levels. Also, the function of producing these reports is only available at the system administrator level.

In determining the “unusual, successful access,” the system determines unusual access against the Clinics’ hours of operation as defined in the appointment scheduler. Note: This infers what hours of operation for a Clinic will be when the doors are open. This issue cuts across functional areas.

Maintain Record Audit

The transfer system records the User ID and date of creation for all data in all tables in the system. Additionally, any data that is updated has the User ID and date also recorded in a separate column from the creation User ID and date. It should be noted that only the last person updating the record will have their User ID and date recorded as all previous entries will be overwritten.

Limit Unauthorized Access

The AIM System invokes a Windows-based window saver if a terminal goes unused for a set period of time. To get back into the application, the User must enter a User ID and password through a message box facility.

The system will also log off any workstation that has not been utilized for a set period of time. This network operating system administration function automatically logs off the User from the network and application. Any information that was entered but not saved will be lost at the workstation in question.

Other Security Measures

The system employs a number of system security measures:

- The system restricts User access to data only through programs or approved ad-hoc tools.

- The system restricts User access to data by function. The system includes a recovery and restart procedure for application software in the event of errors.
- All data electronically transmitted by the system is encrypted by the sending station before transmission and decrypted by the receiving station upon receipt of transmission.

Archive System Data

WIC Program requirements stipulate that various types of records be kept for a number of years. To satisfy this requirement while preserving efficient system operation, it is necessary to remove information that is not required for day to day processing in the WIC System. Historical WIC data can be stripped from the system and stored off-line (archived) for potential future use.

Archive Historical Data

The AIM System archives historical WIC participant and vendor records according to parameters specified by the State Agency. It is possible to specify different time periods for different types of records since it is important to retain some types of data for longer time periods than others. The system builds a table that informs a User that a record was previously stored in the system and is now located in the system archives. The AIM System can retrieve those files for User access within 24 hours, upon request. Operating procedures will be established at Local agencies and Clinics to request retrieval of this information so that participants are not turned away because their files are not available on-line.

As records are archived, an index is created and updated containing the participant identification, name and date of archival. This indexing allows for selective retrieval from the archive tape by participant. An archival report is also printed listing the index. This index report is safely stored along with the appropriate archive tape.

Retrieval of Historical Data

The system provides the capability of retrieving historical data from archive and restoring it. Users can request participant data by ID, name, Local Agency, Clinic and/or archive date, or vendor data by ID, name, and/or archive date and have it restored at the State Agency server and transported via the end of day process.

Retrieval from archive is a system function that, in most cases, is available on an overnight basis at the State server. If the data to be retrieved from archive spans multiple archive tapes, Users are asked to load the appropriate tape for items to be retrieved. Each tape is individually requested by the operating system.

Data retrieved from archive is sent to the appropriate Local Agency server utilizing the end of day process. Since purging is done at both the Local and State Agency but the purging at the State Agency is driven by the archival process (and purging at the local level is driven by the end-of-day process), a method has been devised so that there will be data synchronization between the Local and State Agency databases. This method consists of the transfer of a file of state archived participants and vendors down to the agencies via end of day. This file triggers a process which removes these same participants and vendors from the Local Agency databases.

Purge Unnecessary Data

This process is identical to the archive process described above, with the exception that the data is not stored before it is stripped from the system. State agencies may collect some types of information that are of no use after the period that they are needed on-line. The system will allow this information to be purged completely.

The System Administration function is where purge criteria is defined and purging functions are run. Purging functions will be run on an ad-hoc basis as system resources become available at the time an archive is requested. It should be noted that archiving is a State server function while purging will be done at both the State and Local Agency servers.

The WIC System will purge all data that has been unused for a User-specified length of time. This will occur as a normal part of the archive process.

Maintain Archive Parameters

The system provides defaults for determining the inactive period at which data is to be archived (66 months for participant data, 999 months for vendor data). It is also necessary to provide the capability to change these values on an ad-hoc basis. The system allows Users to enter these values whenever data is archived.

Administer Backup/Restore

The AIM System provides the WIC Systems Administrator with the ability to administer backup and restore procedures in the most simple and effective method possible.

Provide Central System Backup Capability

Backup functions will be provided for the Central database. This function will be executable from the menu and will have User selectable options that define the content of databases, directories, and files that the system will backup.

On a daily basis, the system administrator will backup the system to tape. The administrator will be able to define the type of backup to perform including daily, monthly, yearly or custom. Each of these backups will have a different set of files and directories associated with it. The backup function will be executable from the Central server and be an integrated part of the end of day process. The backup process will also be executable as a separate menu item. Restoring the backup must be done manually.

Because backup tapes are most likely reused following a father-grandfather rotation, they should not be used for archiving. It is recommended that archive tapes be placed in storage and never reused as it will be the only copy containing particular data.

Provide Local Agency System Backup Capability

Backup procedures at the Local Agency will function in a similar manner to that utilized on the Central server. Backups will normally be run through the end of day process, but a User selectable backup process will also be included on the menu at Local agencies.

Note: It will be the responsibility of Users or local

administrators to backup their own workstation.

Administer End of Day

The End of Day process initiates a number of processes and reports for the Agency/Clinic. The local administrator uses a simple window from which all of these processes are run. These processes can not be individually run from this area. The window prompts the User for three distinct items to have been completed before the End of Day process is initiated. These are: Verify that the Clinic functions are completed for the day, verify that the printers are on and are loaded with paper, and verify that the backup tape has been loaded in the server. Once the User initiates the process, it proceeds automatically, and no User intervention is required from this point forward. The backup and end of day processes will proceed during the evening and produce outputs for staff members to review on the following business day.

Process End of Day Activities

The End Of Day (EOD) activities assist in the movement of data throughout the automated WIC System. Additionally, EOD activities backup important data files, and produce status logs to assist the system administration (a complete list is shown below).

Central

Ctrl_sql.log - A list that details by date the participants at each Agency whose records were added, deleted or updated. This includes information regarding the processing of food instruments.
Sql.log - A historic list that details by date the participants at each Agency whose records were added, deleted or updated.
Ec.log - A list that details by date and time that all Central Agency scripts initiated and finished.
Ec_his.log - A historic list that details by date and time that all Central Agency scripts initiated and finished.
Mon_bank.log - A historic log file that details by date and time the scripts are initiated and completed to transfer information back and forth between the Central Database and the Banking Intermediary.
Agcy_01.log - This script details for a single Local Agency (in this case 01) the table data that was extracted from the Agency's base tables, updated at the Central server, then exported from the Central server database.
Agcy_01_his.log - This script is a historic log which details for a single Local Agency (in this case 01)the table data that was extracted from the Agency's base tables, updated at the Central server, then exported from the Central server database.
01_ec4_retrieve.log - This scripts details that the scripts concerning retrieving and storing requested archived data at the Central Database have run.

Local Agency

Ea.log - This script details by date and time that outputs at the Local Agency have printed.
Mon_agcy.log - This is a historic log that details by date and time that connections and file transfers were successful to and from the Central Server database.
Agcy_ctrl.log - A list that details inserts of all new and updated data into the End of Day temporary tables. It also provides information regarding the export of these tables for preparing the zip filed to be sent to the Central Server database.

Agcy_sql.log - A list that details participants who have been terminated or experienced a category change during the End of Day process.
Appt_Not.log - Details whether the printing of appointment notices was successful or unsuccessful.
Ctrl_agcy.log - A list that details the transfer of base table, participant, and food instrument data from the Central Server Database to the Agency Server Database.
Agcy_01.log - A historical log that details for the Agency the data that was extracted from the Agency's base tables and exported to the central server.
EC4_DUAL - This report prints out at each Local Agency detailing the Participant ID, Name, Birth Date, Category, Address and Phone Number of Participants who are showing a dual enrollment in the AIM system.
Ineligibility Notices - The system prints out a letter for each participant who has been determined ineligible through the end of day process.
Appointment Notices - The system prints out a letter for each participant who is scheduled to have a WIC / CSFP appointment in 14 days.
Appointment Labels - The system generates a mailing label for each Appointment notice letter generated.
CSF Notice to Reapply - The system generates a letter for each participant who must reapply for CSF because their eligibility will end in 6 weeks.

Administer External System Interfaces

The AIM System must interface with other systems by providing data for them. One of the functions of this system is to provide data to the Centers for Disease Control and Prevention (CDC) and ABT Associates regarding WIC participant Characteristics, Pregnancy Nutrition Surveillance Data, and Pediatric Nutrition Surveillance Data. This information is transferred to the CDC and ABT Associates in methods prescribed by Federal Requirements for each of them, and are further described below. Each of the reporting interfaces have their own window to generate the specific reporting file of information.

Generate Participant Characteristics Information

The Participant Characteristics Report File is generated to meet Federal reporting requirements, and is transmitted via magnetic tape. The User produces the report (usually in April) by entering the month for which they wish to generate the report. This report is then generated to the tape and can be submitted to ABT Associates (a federal contractor) for final submission to the CDC.

Generate Pediatric Nutrition Surveillance Information

The Pediatric Nutrition Surveillance Report (PEDS) is generated to meet federally required reporting regarding pediatric participant characteristics. This information is then output to a file for input to the EPI Info System, or written to magnetic tape for submission to the CDC. The Systems Administrator must select which output type s/he desires, and if it is for the EPI Info System, s/he must enter the filename to be created. Once the output is selected, the User must enter the month for which the report will be generated. This is all done from one window.

Generate Pregnancy Nutrition Surveillance Information

The Pregnancy Nutrition Surveillance Information Report (PNSS) is generated to meet federally required reporting regarding pregnant participant characteristics. This information is then output to a file for input to the EPI Info System, or written to magnetic tape for submission to the CDC. The Systems Administrator must select which output type s/he desires, and if it is for the EPI Info System, s/he must enter the filename to be created. Once the output is selected, the User must enter the quarter for which the report will be generated. This is all done from one window.

Administer Data Transfer Between Satellite Clinics and Local Agencies

When a Satellite Clinic is held, it is necessary to load data from the Local Agency Database to the Satellite Clinic laptop computer. This is done through a process commonly referred to as "checking out" the data. This process protects participant data from corruption/lack of synchronization, and allows the Clinic to operate as if it had a database server with it. Once the Clinic has been completed, the updated data can then be "checked in" to the Local Agency database from the laptop. This data will then in turn update the State Agency's database through the next end of day process.

Administer Load/Unload of Clinic Data

The system allows the User to load data necessary to support mobile laptop functionality, and to enable the Local Agency to perform satellite Clinics at remote sites.

The same mechanism is used to unload or "check in" data.

Manage Satellite Clinic Data

The system will provide for laptop administration at the Local agencies

At the Local Agency server, a function will be provided to temporarily remove the "checked out" flag if for some reason data needs to be updated for a Clinic that is currently on the laptop. It should be noted that Local Agency personnel are responsible for understanding the ramifications of removing this flag and performing data manipulation functions on data that is under the control of laptops in the field.

Note: The Notebook Administration functions are still in development, once code is completed details will be added to this and the above sections.

Provide Management Reports

The AIM System will provide time management reports on the security aspects of the application. These reports are provided to assist site administrators in maintaining security.

WIC Role Authorities

The purpose of this report is to provide the system administrator with a breakdown of the currently established roles, the tables that each role has access to, and the privileges of each table.

WIC User Directory

The purpose of this report is to provide a listing of all current WIC/CSFP Users, their associated roles, and their password expiration dates. This will provide the system administration, and any required supervisors, with the ability to create and view a hard copy report of all Users.

WIC User Access

The AIM System will monitor and list all Users whose password has expired. The purpose of this is for the administrator to consider deleting the User since the account is not accessible. Unused accounts may propose a security risk.

WIC Active and Inactive Roles

The AIM System will provide a listing of WIC/CSFP roles and reference these roles as “Active” or “Inactive.” This will give the administration a “quick view” capability as to which privileges associated with these roles are entered.

System Access

The AIM System will provide a listing of all accesses to the applications that were denied, and the reason for the denial.

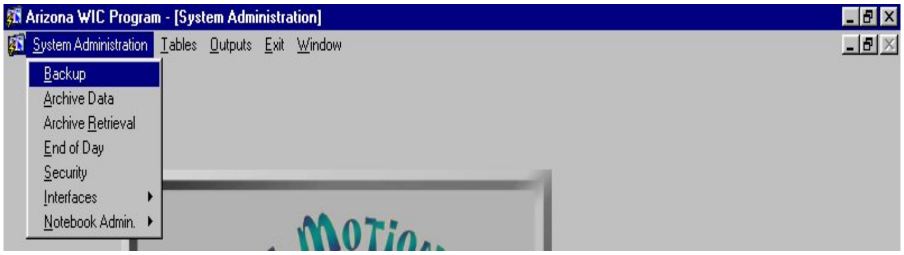
Pending Certification Records

The AIM System allows the User to produce a report detailing the participants entered in the AIM system who have begun the certification process, but have not been issued food instruments. This report is **not** to include Breastfed infants who are scheduled not to receive food instruments.

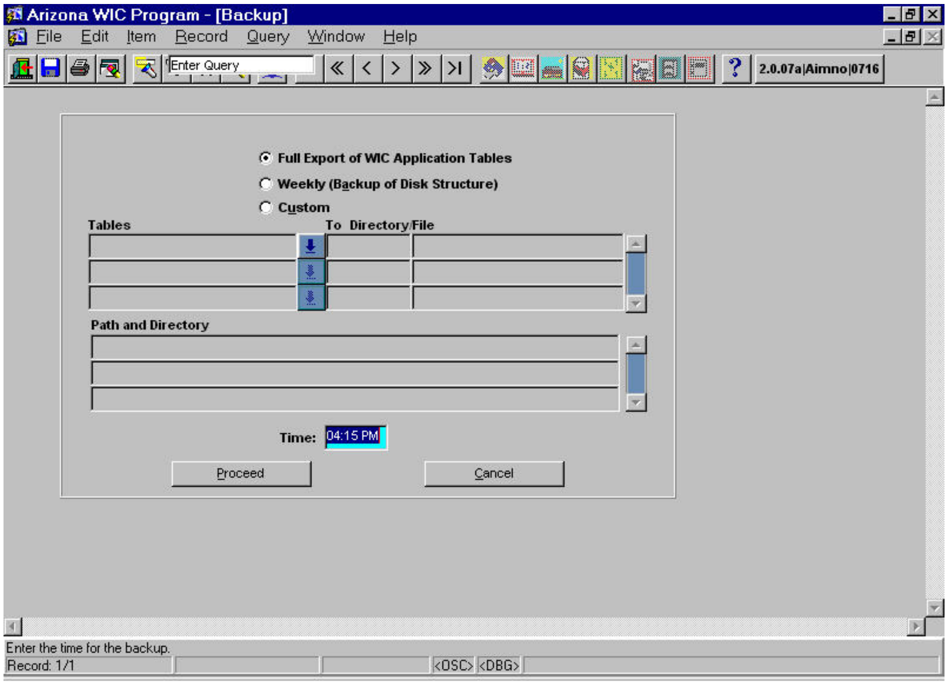
Performing a Backup

To Perform a Backup:

1. Click on System Administration from the menu bar
2. Click on Backup as shown below:



The Backup Window is displayed:



● Full Export of WIC Application Tables
○ Weekly (Backup of Disk Structure)
○ Custom

Time: 04:15 PM

Enter the time for the backup.
Record: 1/1

Figure 1 - Backup

Perform Backup

1. Select whether you want a Full Export, Weekly or Custom backup by clicking once on the radio button next to that type of backup.
2. TAB to the Time field, then type the time you want the backup processing to begin in the following format: HH:MM AM or HH:MM PM.
3. Click the Proceed button to initiate the Backup process, or Click the Cancel button to exit the screen.

Perform a Custom Backup

1. Select the Custom backup by clicking once on the radio button next to the Custom field.
2. Click the list of values button to the right of the first blank under the Tables field.
3. Select the table that you want to backup by double clicking on the name of the table.
4. Tab to the Path and Directory field. Enter the Path and Directory name you want the table backup to be stored in.
5. If you want to select another Table to backup, click the next available blank space under the Tables field.
6. Click the list of values button next to that space and select the table that you want to backup by double clicking on the name of the table.
7. Repeat Step 4.
8. TAB to the Time field, then type the time you want the backup processing to begin in the following format: HH:MM AM or HH:MM PM.
9. Click the Proceed button to initiate the Backup process, or Click the Cancel button to exit the screen.

Fields

Tables - Enter tables to be backed up (custom selection only). This field contains a list of values that is selected and maintained by the User. This field is optional.
Directory/File - Enter directory/files to be backed up (custom selection only). This field is display only.
Path and Directory -
Time - The time of the day that the system backup is to begin. This field is mandatory and must be entered when the User chooses to schedule the backup for a later time. The time entered must be in the future.

Radio Button(s)

Full Export of WIC Application Tables - When selected, a backup of all WIC Tables will be performed.
Weekly - When selected, a weekly backup of the file system is performed.
Custom - When this button is selected, the User may choose what tables and files to back up.

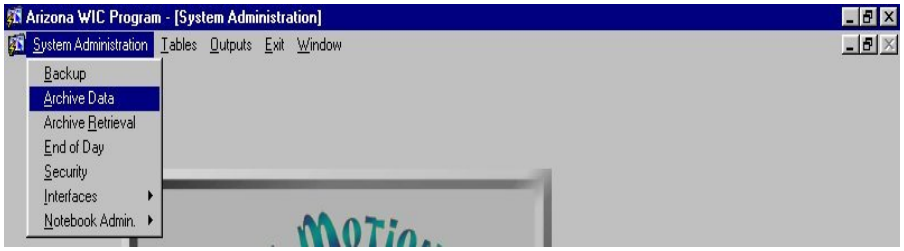
Push Button(s)

Proceed - Click on this button to initiate the backup process.
Cancel - Click on this button to cancel/exit the Window.

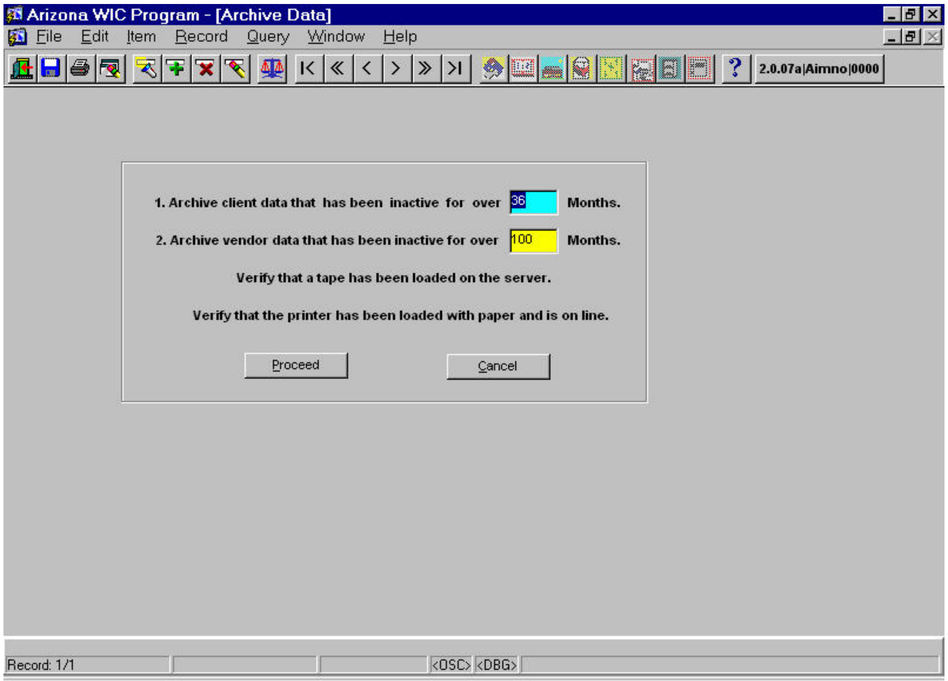
Archiving Data

To initiate Archive Processing:

1. Click on System Administration from the menu bar.
2. Click on Archive as shown below:



The Archive Data screen is displayed:



1. Archive client data that has been inactive for over 36 Months.

2. Archive vendor data that has been inactive for over 100 Months.

Verify that a tape has been loaded on the server.

Verify that the printer has been loaded with paper and is on line.

Figure 2 – Archive Data

Initiate Archive Processing

1. Tab to item 1 if looking to archive client data.
2. Type in the number of months for which inactive client data is desired to be archived.
3. Tab to 2 if looking to archive vendor data.
4. Type in the number of months for which inactive vendor data is desired to be archived.

Fields

1. The age, in months, of inactive participant records to be archived. Any inactive participant

and participant related records of that age or older will be archived. This field is mandatory.
2. The age, in months, of inactive vendor records to be archived. Any inactive vendor records of that age or older will be archived. This field is mandatory.

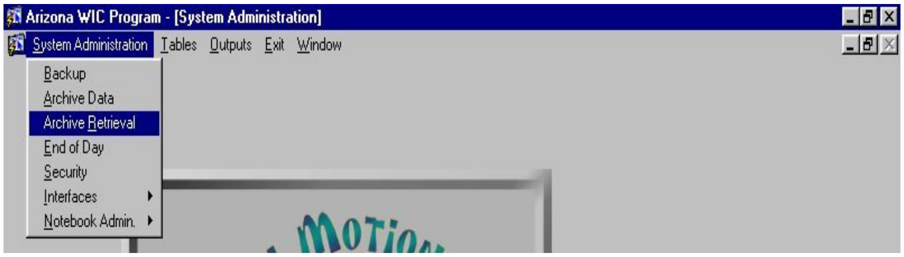
Push Button(s)

Proceed - Click on this button to initiate the archive process.
Cancel - Click on this button to cancel/exit the Window.

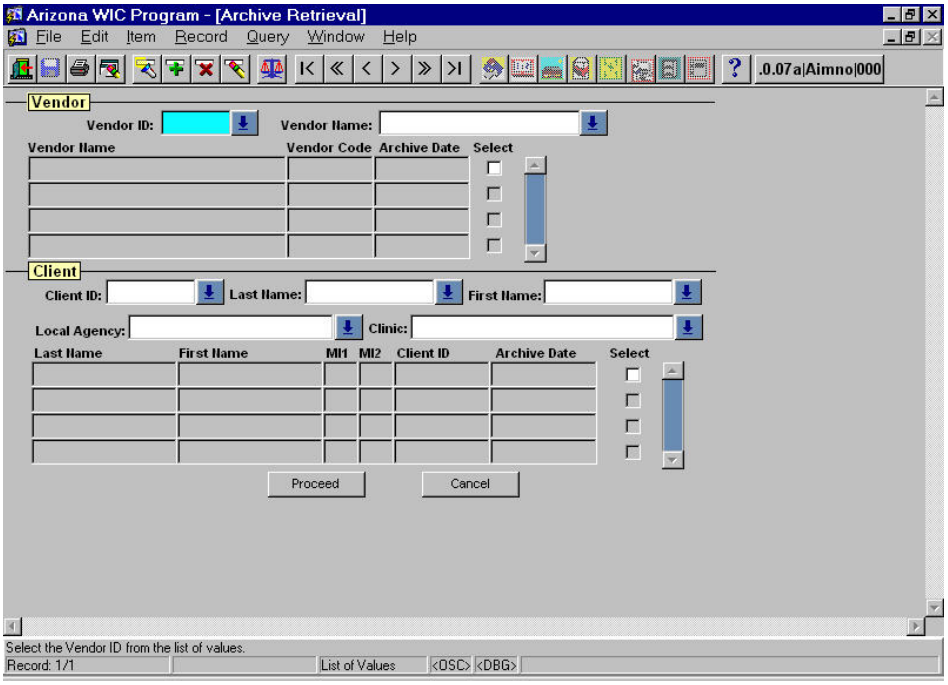
Perform Archive Retrieval

To initiate Archive Retrieval:

1. Click on System Administration from the menu bar.
2. Click on Archive Retrieval as shown below:



The Archive Retrieval screen is displayed:



Select the Vendor ID from the list of values.
Record: 1/1

Figure 3 – Archive Retrieval

Initiate Archive Retrieval of Vendor Data

1. Type in Vendor ID (or double click to perform a vendor lookup) and/or the vendor name if vendor info is desired to be retrieved.
2. Execute the query by selecting F8, or selecting execute query from query in pull down list.
3. The vendors that match the selected criteria will appear in the results section.
4. Check the select check box for any vendors for which to retrieve archived information.

5. Click the proceed button to initiate the Archive process, or click the cancel button to exit the screen.

Initiate Archive Retrieval of Client Data

1. Type in Client ID (or double click to perform a Client lookup) and/or the client name if client info is desired to be retrieved.
2. Execute the query by selecting F8, or selecting execute query from query in pull down list.
3. The clients that match the selected criteria will appear in the results section.
4. Check the select check box for any clients for which to retrieve archived information.
5. Click the proceed button to initiate the Archive process, or click the cancel button to exit the screen.

Fields

The following fields are used as parameters that determine which vendors or participants are shown in the scrollable blocks of the window.

Vendor ID - The identification associated with the vendor data to be restored from archive files. This field is only entered if vendor data is to be retrieved by searching for a specific vendor ID.
Vendor Name - The name of the vendor retail outlet as it was captured during the authorization process. This field is only entered if vendor data is to be retrieved utilizing the outlet (vendor) name.
Client ID - The identification associated with the participant data to be restored from archive files. This field is only entered if the participant data is to be retrieved utilizing a specific participant ID.
Last Name - The last name of a participant who may need to be retrieved from archive. This field is only entered if the participant data is to be retrieved utilizing a specified name.
First Name - The first name of a participant who may need to be retrieved from archive. This field is only entered if the participant is to be retrieved utilizing a specified name.
Local Agency - The Local Agency of the participant(s) who may need to be retrieved from archive. This field is only entered if the participant is to be retrieved utilized the specified Local Agency to receive WIC services.
Clinic - The Clinic of the participant (s) who may need to be retrieved from archive. This field is only entered if the participant (s) to be retrieved utilized the specified Clinic to receive WIC services.

The following fields represent the results of entered parameter values:

Vendor Name - The name of the vendor retail outlet as it was captured during the authorization process. This field is display only.
Vendor Code - The identification number associated with the vendor name returned. This field is display only.
Archive Date - The date that this vendor’s information was placed into archival storage. This field is display only.
Last Name - The last name of a client who may need to be retrieved from archive. This field is display only.
First Name - The first name of a client who may need to be retrieved from archive. This field is

display only.
MI 1 - The first middle initial of a client who may need to be retrieved from archive. This field is display only.
MI 2 - The second middle initial of a client who may need to be retrieved from archive. This field is display only.
Client ID - The identification of a client who may need to be retrieved from archive. This field is display only.
Archive Date - The date that this client information was placed into archival storage. This field is display only.

Push Button(s)

Proceed - Click this button to initiate the archive retrieval.
Cancel - Click this button to cancel/exit this window.

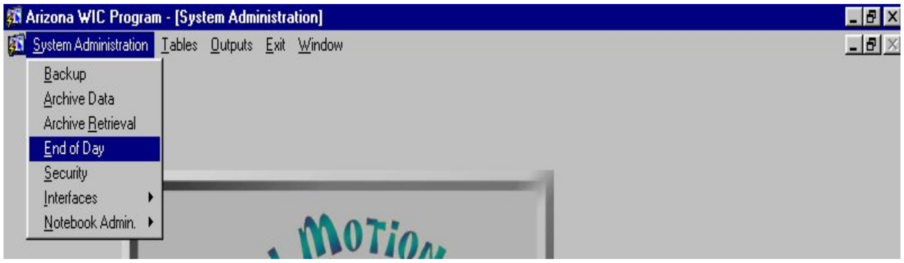
Check Boxes

Select (Vendor) - "X" by clicking on the box to select desired vendor retrieval parameters.
Select (Client) - "X" by clicking on the box to select desired client retrieval parameters.

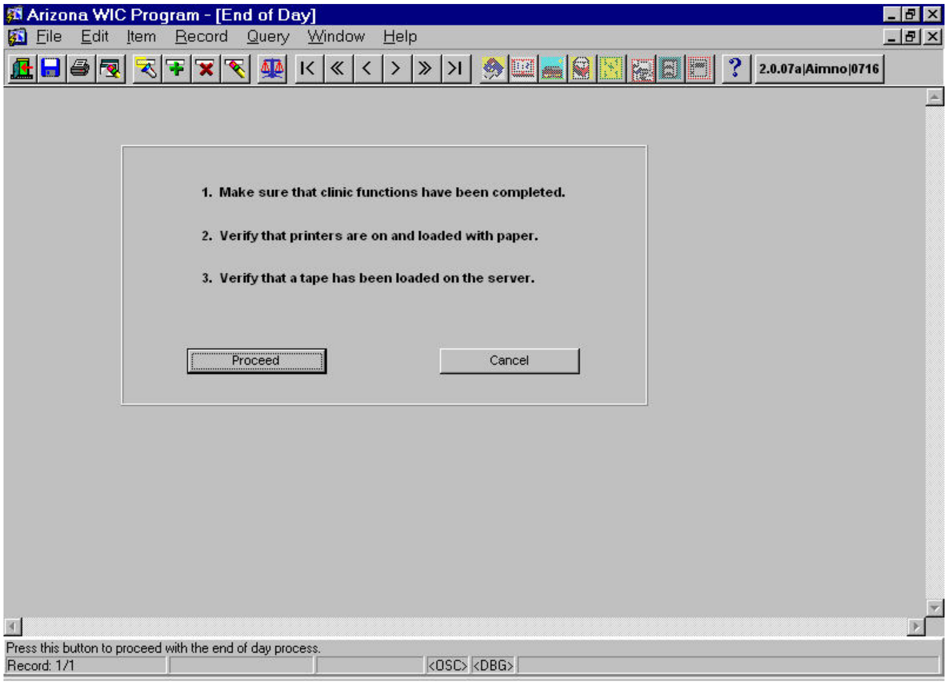
Initiating End of Day Processing

To Initiate End of Day Processing:

1. Click on System Administration from the menu bar.
2. Click on End of Day as shown below:



The End of Day Window is displayed:



1. Make sure that clinic functions have been completed.

2. Verify that printers are on and loaded with paper.

3. Verify that a tape has been loaded on the server.

Press this button to proceed with the end of day process.

Record: 1/1

Figure 4 - End of Day

Initiate the End of Day Processing Procedures

1. Perform steps 1-3 in the End of Day Window.
2. Click the Proceed button to begin the End of Day processing, or Click the Cancel button to exit the screen.

Fields

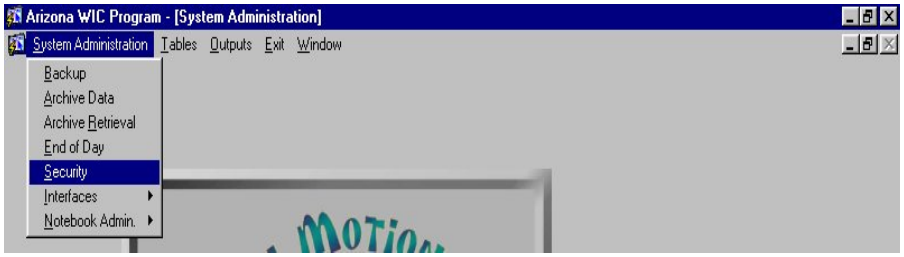
Push Button(s)

Proceed - Click on this button to initiate the End of Day processing.
Cancel - Click on this button to cancel/exit the Window.

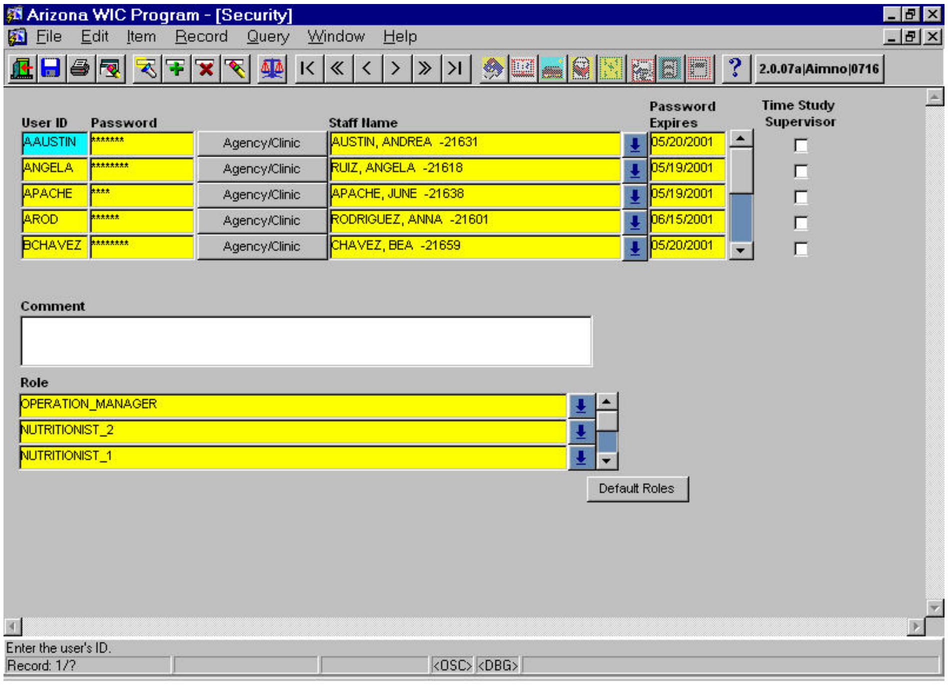
Maintaining Security

To Maintain Security:

1. Click on System Administration from the menu bar.
2. Click on Security as shown below:



The Security window is displayed:



User ID	Password		Staff Name	Password Expires	Time Study Supervisor
AAUSTIN	*******	Agency/Clinic	AUSTIN, ANDREA -21631	05/20/2001	□
ANGELA	********	Agency/Clinic	RUIZ, ANGELA -21618	05/19/2001	□
APACHE	****	Agency/Clinic	APACHE, JUNE -21638	05/19/2001	□
AROD	******	Agency/Clinic	RODRIGUEZ, ANNA -21601	06/15/2001	□
BCHAVEZ	********	Agency/Clinic	CHAVEZ, BEA -21659	05/20/2001	□

Comment

Role

OPERATION_MANAGER
NUTRITIONIST_2
NUTRITIONIST_1

Default Roles

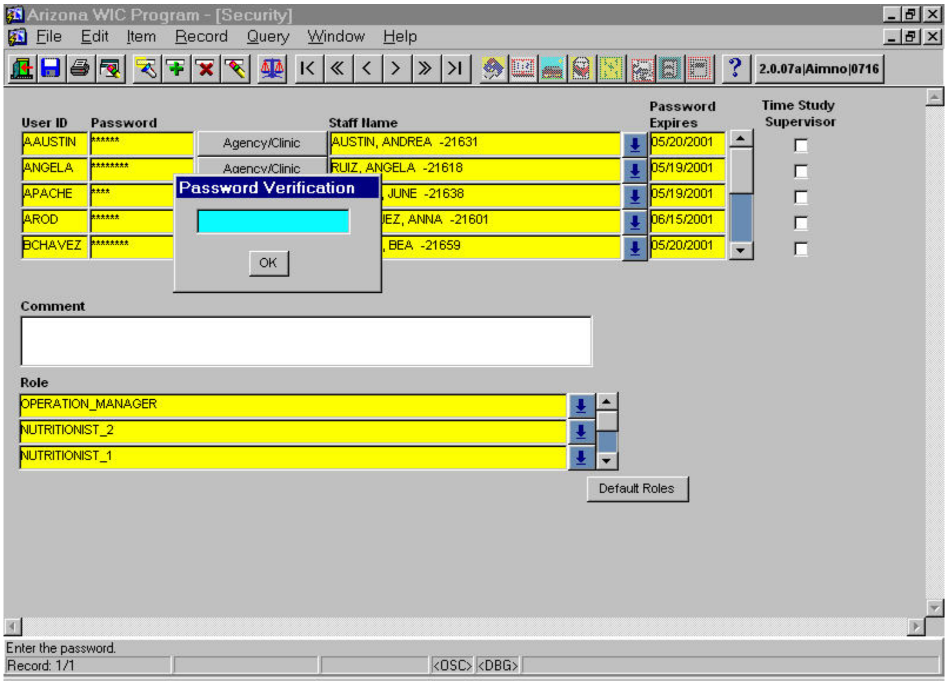
Enter the user's ID.
Record: 1/? <OSC> <DBG>

Figure 5 - Security

Add a WIC User and Assign a Role

1. Click in a blank row or click the green plus icon to insert a blank row.
2. Enter the User ID for the new WIC/CSFP User desired.
3. TAB to the Password field, then enter the password to be assigned to this new ID. The minimum length for a password is four (4) alphanumeric characters. The maximum length for a password is eight (8) alphanumeric characters. Only alphabetic, numeric or a combination of these two can be entered as a password. No other character is allowed. The system will show an asterisk (*) for every character because it automatically encrypts the password entered.

4. Press the Enter or TAB key. The following pop-up window will appear:


Arizona WIC Program - [Security]
File Edit Item Record Query Window Help
2.0.07a|Aimno|0716
Agency/Clinic
Agency/Clinic
OK
Default Roles
<OSC> <DBG>

User ID	Password	Staff Name	Password Expires	Time Study Supervisor
AAUSTIN	******	AUSTIN, ANDREA -21631	05/20/2001	□
ANGELA	********	RUIZ, ANGELA -21618	05/19/2001	□
APACHE	****	, JUNE -21638	05/19/2001	□
AROD	******	EZ, ANNA -21601	06/15/2001	□
BCHAVEZ	********	, BEA -21659	05/20/2001	□

Password Verification

Comment

Role

OPERATION_MANAGER

NUTRITIONIST_2

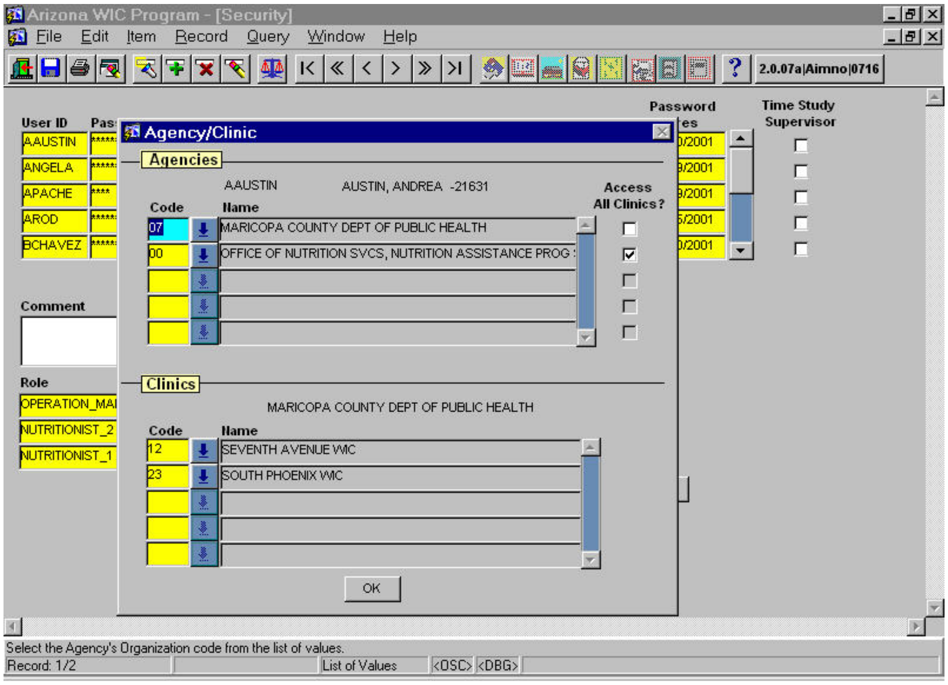
NUTRITIONIST_1

Enter the password.

Record: 1/1

Figure 6 - Password Verification Pop-Up

5. Type in the Password again to verify it. Click OK to return to the Security window.
6. Click the list of values button to the right of the Staff Name field, then select the last name of the staff member to be assigned to this new WIC/CSFP User ID and Password by double clicking on the name.
7. TAB to the Password Expires field, the system defaults to (8) eight days from today’s date. The date may be modified within (1) one week of the current date only.
8. Check the Time Study Supervisor checkbox if the User is a Time Study Supervisor.
9. Click the Agency push button. The following pop-up window will appear:



AAUSTIN
ANGELA
APACHE
AROD
BCHAVEZ

OPERATION_MAI
NUTRITIONIST_2
NUTRITIONIST_1

AAUSTIN AUSTIN, ANDREA -21631

Code	Name	Access All Clinics?
07	MARICOPA COUNTY DEPT OF PUBLIC HEALTH	□
00	OFFICE OF NUTRITION SVCS, NUTRITION ASSISTANCE PROG	☑
		□
		□
		□

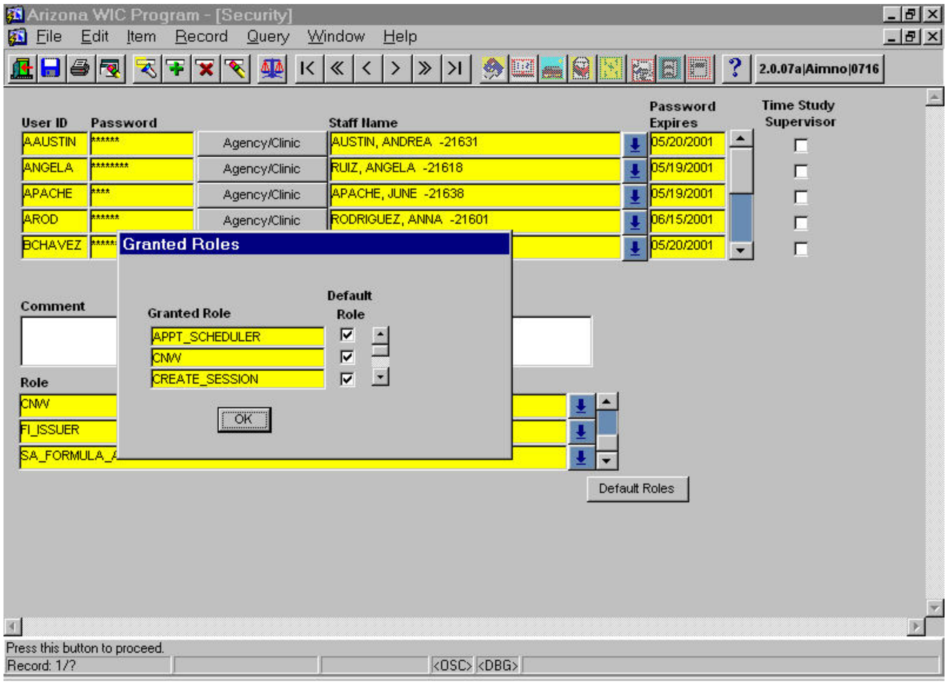
MARICOPA COUNTY DEPT OF PUBLIC HEALTH

Code	Name
12	SEVENTH AVENUE WIC
23	SOUTH PHOENIX WIC

Select the Agency's Organization code from the list of values.
Record: 1/2 List of Values <OSC> <DBG>

Figure 7 - Agency Pop-Up

10. Click the list of values button to the right of the Code field, then select the Agency with which to associate this User by double clicking the Agency name. To assign more than one Agency to this User, press the down arrow key once, then enter the name of the next Agency. Click OK to return to the Security window.
11. TAB to the Role field. Click the list of values button to the right of the Role field, then select the role with which to associate this User by double clicking the Role name. If more than one role is to be assigned to this new User, press the down arrow key once, then enter the name of the next role.
12. Click the Default Roles push buttons. The system will display a pop-up window indicating "Do you want to change default roles to the User?" By selecting Yes, the Granted Roles pop-up window will appear:


Arizona WIC Program - [Security]
File Edit Item Record Query Window Help
2.0.07a|Aimno|0716
Agency/Clinic
Default Roles
Granted Roles
OK
Press this button to proceed.
Record: 1/?
<OSC> <DBG>

User ID	Password		Staff Name	Password Expires	Time Study Supervisor
AAUSTIN	******	Agency/Clinic	AUSTIN, ANDREA -21631	05/20/2001	□
ANGELA	********	Agency/Clinic	RUIZ, ANGELA -21618	05/19/2001	□
APACHE	****	Agency/Clinic	APACHE, JUNE -21638	05/19/2001	□
AROD	******	Agency/Clinic	RODRIGUEZ, ANNA -21601	06/15/2001	□
BCHAVEZ	*****			05/20/2001	□

Comment

Role: CNW, FI_ISSUER, SA_FORMULA_A

Granted Role	Default Role
APPT_SCHEDULER	☑
CNW	☑
CREATE_SESSION	☑

Figure 8 - Granted Roles Pop-Up

13. In order to have these roles granted to the User each time they log on, click the check box corresponding to the Granted Role(s). Otherwise, the default is to Not Granted.
14. Click the OK button to return to the Security window.
15. Click the Save icon. The system will display a pop-up window indicating: “Transaction Completed”. Click on the OK button and a new WIC/CSFP User has successfully been added into the system.

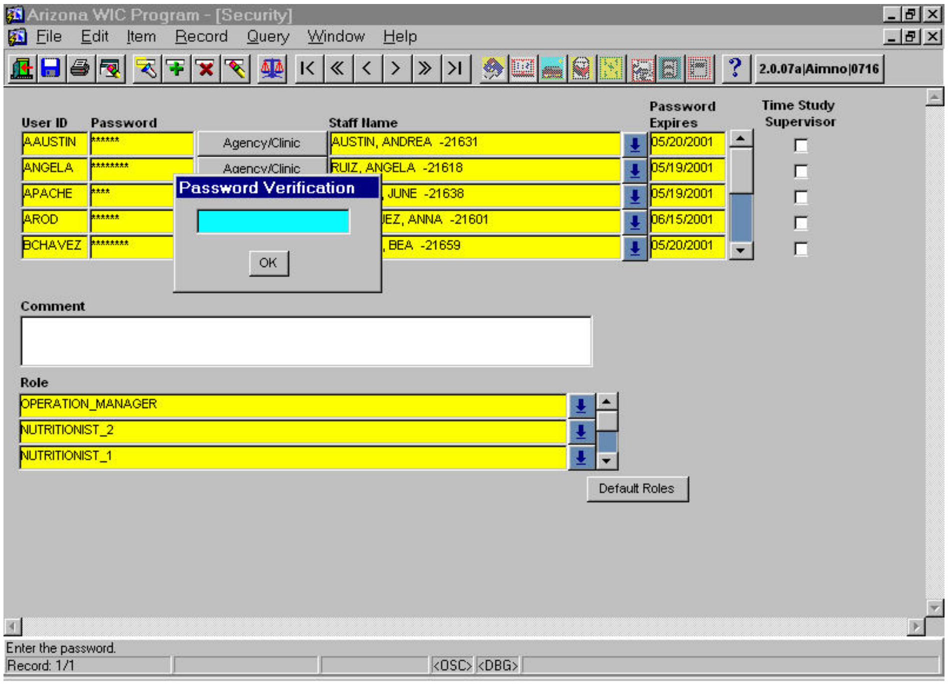
Update a WIC User

There are several methods to update a User. One way is to change their password. Another way is to modify the agencies the User can logon to.

Note: If the User logs on at the State level, s/he will be able to change User roles so that any User will be able to logon to any Agency. If the User logs on at a specific Agency, s/he will only be able to add that Agency to any of the Users.

To Change Password:

1. Click in the Password field to change. Remove the old password using the backspace key or by selecting the item “clear” from the Edit pull down menu.
2. Type in the new unique Password. Press the Enter or TAB key. The following pop-up will appear:


Arizona WIC Program - [Security]
File Edit Item Record Query Window Help
2.0.07a|Aimno|0716
Password Verification
OK
Default Roles
<OSC> <DBG>

User ID	Password		Staff Name	Password Expires	Time Study Supervisor
AAUSTIN	******	Agency/Clinic	AUSTIN, ANDREA -21631	05/20/2001	□
ANGELA	********	Agency/Clinic	RUIZ, ANGELA -21618	05/19/2001	□
APACHE	****		, JUNE -21638	05/19/2001	□
AROD	******		EZ, ANNA -21601	06/15/2001	□
BCHAVEZ	********		, BEA -21659	05/20/2001	□

Comment

Role
OPERATION_MANAGER
NUTRITIONIST_2
NUTRITIONIST_1

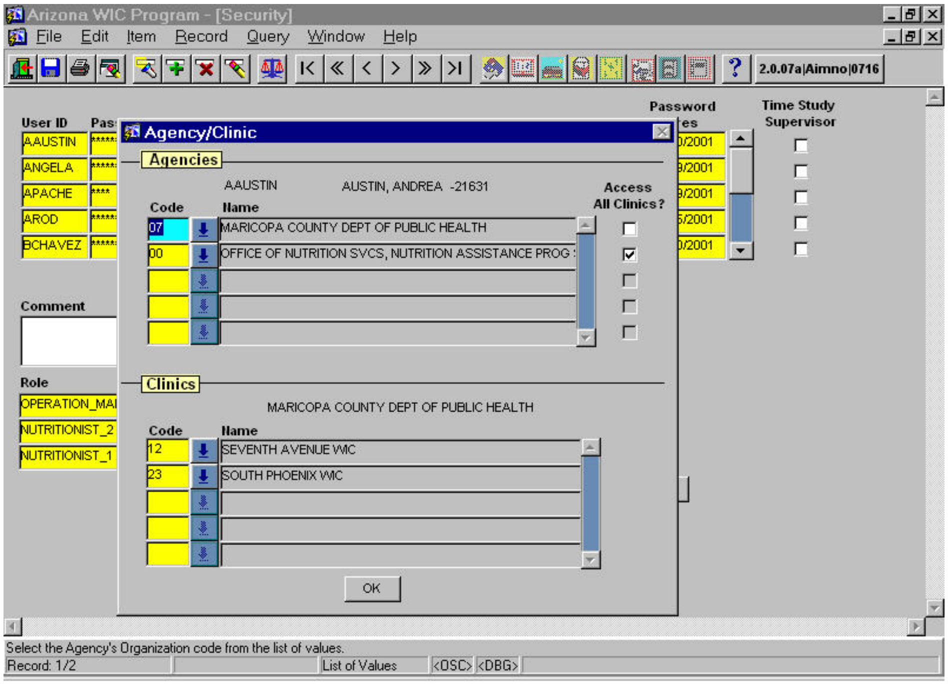
Enter the password.
Record: 1/1

Figure 9 - Password Verification Pop-Up

3. Type in the new Password again to verify it. Click OK to return to the Security window.
4. Click the Save icon.

To modify Agency access

1. Click the Agency push button corresponding to the User to update. The following pop-up window will appear:


Arizona WIC Program - [Security]
File Edit Item Record Query Window Help
2.0.07a|Aimno|0716
OK

User ID	Pas
AAUSTIN	*****
ANGELA	*****
APACHE	****
AROD	*****
BCHAVEZ	*****

Password
Time Study Supervisor

Comment

Role
OPERATION_MAI
NUTRITIONIST_2
NUTRITIONIST_1

Agency/Clinic

Agencies

AAUSTIN AUSTIN, ANDREA -21631

Code	Name	Access All Clinics?
07	MARICOPA COUNTY DEPT OF PUBLIC HEALTH	☐
00	OFFICE OF NUTRITION SVCS, NUTRITION ASSISTANCE PROG	☑
		☐
		☐
		☐

Clinics

MARICOPA COUNTY DEPT OF PUBLIC HEALTH

Code	Name
12	SEVENTH AVENUE WIC
23	SOUTH PHOENIX WIC

Select the Agency's Organization code from the list of values.
Record: 1/2 List of Values <OSC> <DBG>

Figure 10 - Agency Pop-Up

2. To remove an Agency for this User, click the Code field of the Agency. Then click the Remove Record icon.
3. To add more agencies for this User, click the list of values button to the right of the Code Field, then select the Agency with which to associate this User by double clicking on the Agency name.
4. Click the OK button to return to the Security window.
5. Click the Save icon. The system will display a pop-up window indicating: Transaction Completed." Click the OK button.

Delete a WIC User

1. Click the Enter Query icon.
2. Enter the User ID of the WIC/CSFP User to delete, then press the F8 key to execute the query. The system will automatically populate the remaining fields on the screen with the correct information for that User ID.
3. Click the Remove Record icon and the system will automatically clear all the information for that record from the screen.
4. Click the Save icon. The system will display a pop-up window indicating: "Transaction Completed". Click on the OK button and a WIC/CSFP User has successfully been deleted from the system.

Figure 5 - Security

Fields

User ID - The Oracle User ID assigned to the User. This field is mandatory.
Password - The encrypted Oracle password associated with the User ID. This field is mandatory.

Staff Name - A User can select from a list of values from the staff table that associates a person with the User ID/password combination. This field is mandatory.
Password Expires - The date the password associated with the User ID expires. The initial creation of a password must be changed within eight (8) days of the current date. Once the user has changed their password at the logon screen, it will expire in 45 days. This field is mandatory.
Comment - The User may enter comments associated with this Window. This field is mandatory.
Role - These represent pre-defined groups of User privileges to perform certain actions. A User can be assigned to one or more roles. See the associated table for the outlines the roles and their functions. This field is mandatory.

Push Buttons

Agency/Clinic - Clicking on this button allows the User to display the Agency/Clinic Pop-Up window in which the User associates log in privileges for the Staff Member with specific Local Agencies and Clinics.
Default Roles – Clicking on this button allows the User to display the Security – Granted Roles Pop-Up window in which the User can either accept the granted roles assigned or change them.

Check Boxes

Time Study Supervisor - Check this check box if the User is a Time Study Supervisor.

Figure 6 - Password Verification Pop-Up

Fields

Password Verification - Re-entry of the password is mandatory for verification.

Push Buttons

OK - Closes the pop-up window.

Figure 7 - Agency Pop-Up

Fields

Code - The code associated with a specific WIC program. This field is mandatory
Name - The name of the WIC program associated with the selected Code. This field is display only.

Push Buttons

OK - Closes the pop-up window.

Figure 8 - Granted Roles Pop-Up

Fields

Granted Role – The access roles assigned to the User.

Check Boxes

Default Role – If the role is a default for all Users, the check box will be checked.

Push Buttons

OK -

Figure 9 - Password Verification Pop-Up

Fields

Password Verification - Re-entry of the password is mandatory for verification.

Push Buttons

OK - Closes the pop-up window.

Figure 10 - Agency Pop-Up

Code - The code associated with a specific WIC program. This field is mandatory
Name - The name of the WIC program associated with the selected Code. This field is display only.

Push Buttons

OK - Closes the pop-up window.

Load/Unload Clinic

Note: User Instructions for this function will be added once code has been completed.

Load/Unload Laptop

Below are the registry entry icons you can expect to see on a server laptop.

The “nnnnn Server.reg” icon should be double-clicked the first time you log into AIM at a satellite Clinic. “nnnnn” represents the orange “PROPERTY OF ARIZONA DEPARTMENT OF HEALTH SERVICES” tag number on the server laptop.

NOTE: Coconino and Yavapai counties have their own naming system for the icons to be used at a satellite Clinic. Check with your supervisor if you have ANY questions.

The “Docking Station.reg” icon should be double-clicked the first time you log into AIM to connect to the Local Agency server to see clients at a permanent Clinic.

The “Load-Unload Clinic.reg” icon should be double-clicked before logging into AIM to load/unload a Clinic from/to the Local Agency Server.

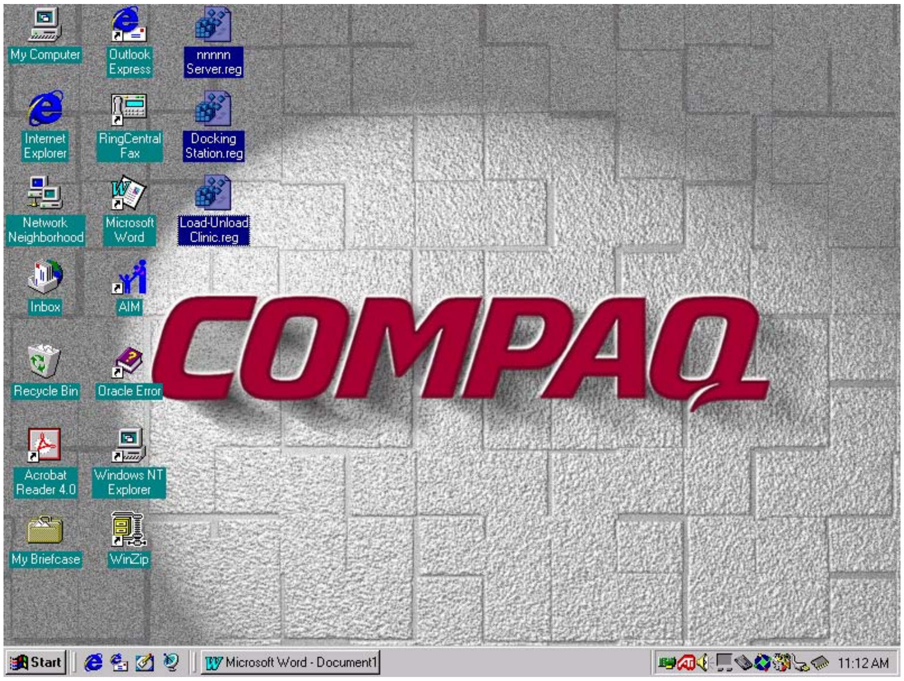


Figure 11 – Desktop, showing Laptop Icons

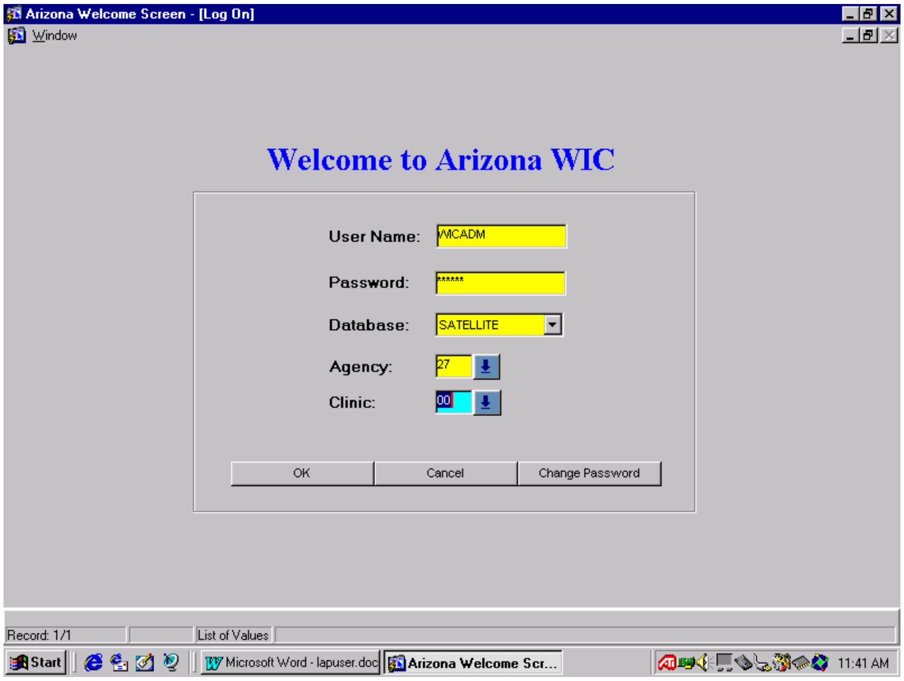
A client laptop will not have the “Load/Unload Clinic.reg” icon since you cannot perform this function on a client laptop. The “Docking Station.reg” icon has the same functionality on a client laptop as on a server laptop.

A client laptop will have “nnnnn Server.reg” icons for every server the client is associated with. For instance, if a client laptop can go out into the field with three different server laptops (at different times, of course), there will be a “nnnnn Server.reg” icon for each server laptop. The Users will need to double-click on the appropriate server icon before entering AIM for the first time.

NOTE: Coconino and Yavapai counties have their own naming system for the icons to be used at a satellite Clinic. Check with your supervisor if you have ANY questions.

Loading a Clinic onto a Satellite Server Laptop:

1. If the laptop is not in the docking station, make sure the laptop is off and then load the laptop into the docking station. Start the laptop by pushing the “power on” button on the right hand side of the docking station.
2. Log into Windows with your designated Username and password. If your Windows logon screen has a domain LOV, select the LOV for your Local Agency. This will update the AIM software to the current version. When the update is complete and the black box goes away, log off.
3. Log into Windows with the Username “administrator” and no password. If your Windows logon screen has a domain LOV, select the domain which corresponds to your orange “PROPERTY OF ARIZONA DEPARTMENT OF HEALTH SERVICES” tag number.
4. Double-click on the “Load-Unload Clinic.reg” icon.
5. Start the AIM system.
6. Using your own AIM Username and password, select SATELLITE from the Database LOV, choose your Local Agency and you MUST select ‘00’ for all Clinics in order to perform the Load Laptop functionality.



User Name: WICADM

Password: ******

Database: SATELLITE

Agency: 27

Clinic: 00

Figure 12 - Login Screen

7. Click on “System Administration” on the AIM Main Menu.
8. From the System Administration dropdown menu, choose Notebook Admin. and then Load/Unload Laptop.

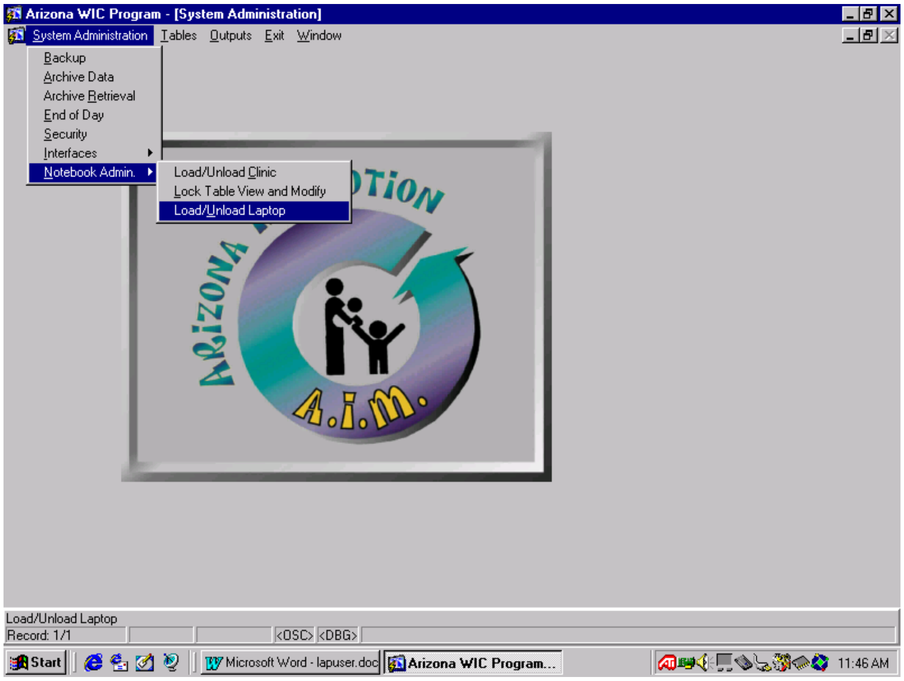


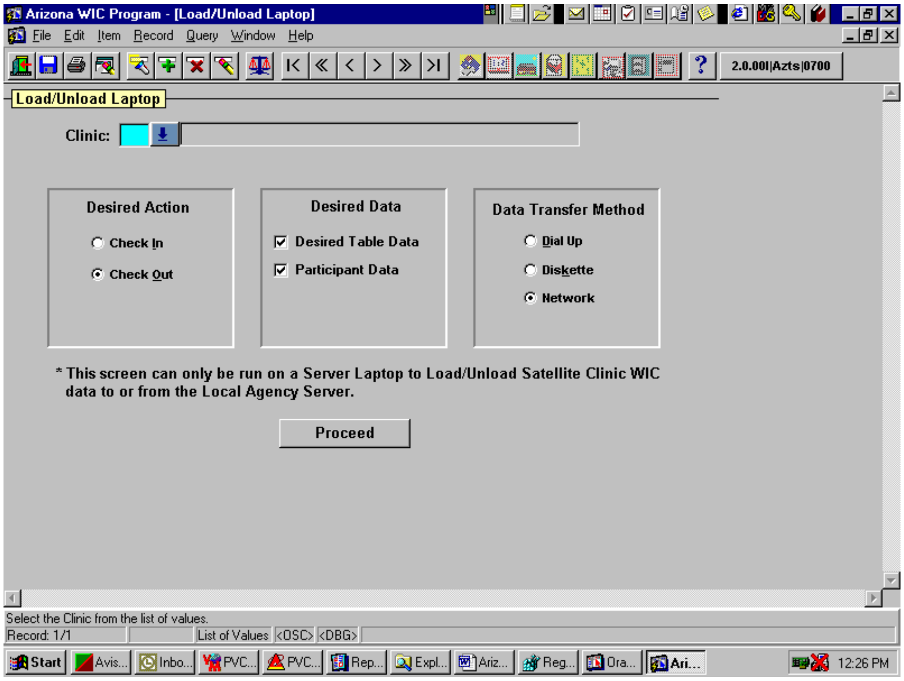
Figure 13 – Menu Path to Load/Unload Laptop

Choose the Clinic you wish to load from the LOV or type in the Clinic code (if you know it) and press <TAB>.

> *Desired Action*: Check Out.
> *Desired Data*: Table Data and Participant Data. This is the default and should never be changed.
> *Data Transfer Method*: Network. This is the default and currently the only functionality enabled in the AIM system.

Press the "Proceed" button. The system will display a series of black boxes which will show the User that the process is running. The process can take 45 minutes to three hours. **NEVER STOP THIS PROCESS WHILE IT IS RUNNING !!!**

If you make a mistake (loading the wrong Clinic on the server laptop, for instance), you MUST let the process continue to completion. Then you can repeat the above steps to load the server laptop with the correct Clinic.



Load/Unload Laptop

Clinic:

Desired Action
○ Check In
● Check Out

Desired Data
☑ Desired Table Data
☑ Participant Data

Data Transfer Method
○ Dial Up
○ Diskette
● Network

* This screen can only be run on a Server Laptop to Load/Unload Satellite Clinic WIC data to or from the Local Agency Server.

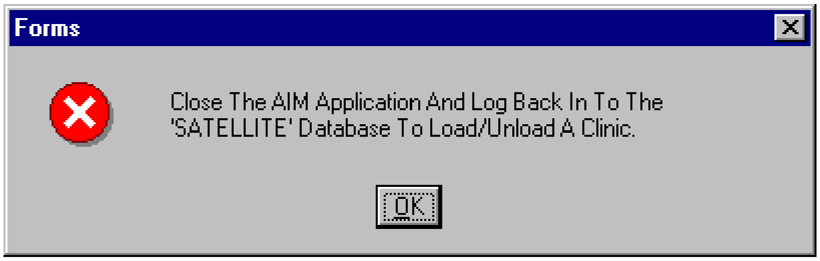
Proceed

Select the Clinic from the list of values.
Record: 1/1 List of Values <OSC> <DBG>

Figure 14 – Load/Unload Laptop

The following are examples of the errors that have been programmed into the software.

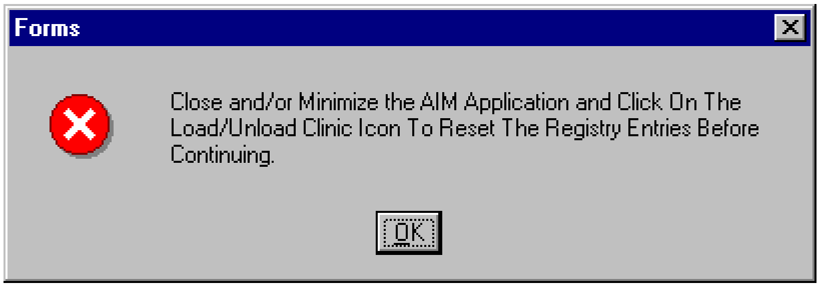
This error will occur if you do not select SATELLITE from the Database LOV on the AZ Logon Screen.



Close The AIM Application And Log Back In To The 'SATELLITE' Database To Load/Unload A Clinic.

Figure 15 - Error Message

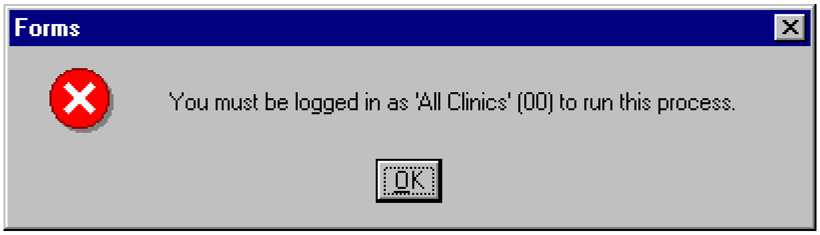
This error will occur if you have not double-clicked on the "Load/Unload Clinic.reg" icon before logging into AIM to do an upload/download.



Close and/or Minimize the AIM Application and Click On The Load/Unload Clinic Icon To Reset The Registry Entries Before Continuing.

Figure 16 - Error Message

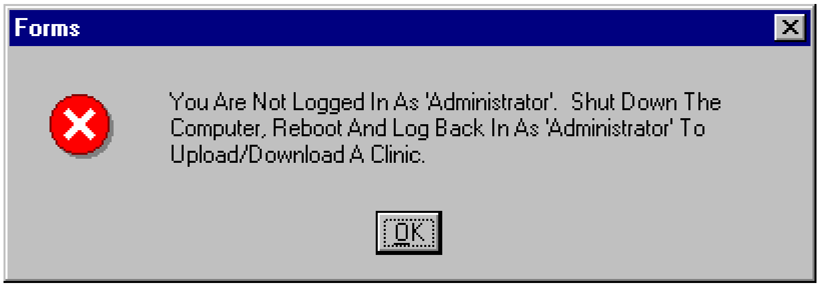
This error will occur if you have not chosen 00 (All Clinics) from the Clinic LOV on the AZ logon screen.



You must be logged in as 'All Clinics' (00) to run this process.

Figure 17 - Error Message

This error will occur if you have not logged into Windows as “administrator”.

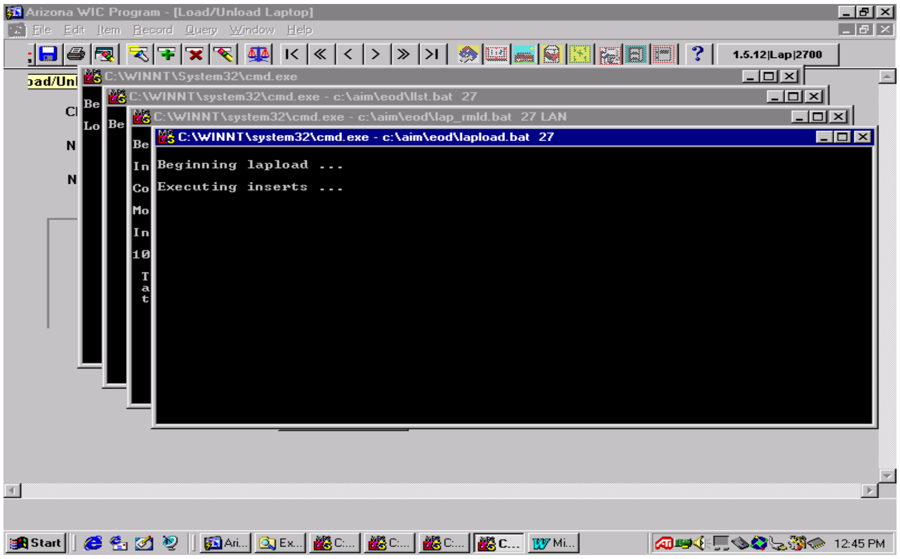


You Are Not Logged In As 'Administrator'. Shut Down The Computer, Reboot And Log Back In As 'Administrator' To Upload/Download A Clinic.

Figure 18 - Error Message

Note: IF ANY OF THESE ERRORS OCCUR, THE LOAD/UNLOAD LAPTOP SCREEN WILL CLOSE AND YOU WILL BE RETURNED TO THE SYSTEM ADMINISTRATION MAIN MENU.

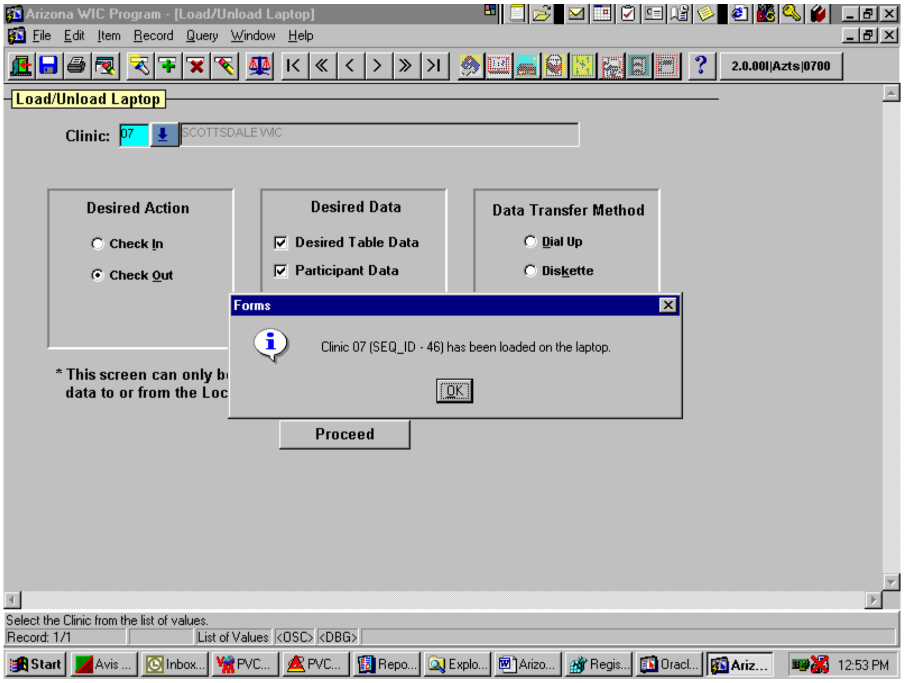
Below is a picture of what the screen will look like while the Clinic is being loaded onto the laptop server. Messages will be displayed to indicate the process' progress.


Arizona WIC Program - [Load/Unload Laptop]
File Edit Item Record Query Window Help
1.5.12|Lap|2700
C:\WINNT\System32\cmd.exe
C:\WINNT\system32\cmd.exe - c:\aim\eod\llst.bat 27
C:\WINNT\system32\cmd.exe - c:\aim\eod\lap_rmld.bat 27 LAN
C:\WINNT\system32\cmd.exe - c:\aim\eod\lapload.bat 27
Start
12:45 PM

```
Beginning lapload ...
Executing inserts ...
```

Figure 19 - MS/DOS Windows

The following message will appear when the laptop server load has successfully completed.



Load/Unload Laptop

Clinic: 07 SCOTTSDALE WIC

Desired Action
○ Check In
● Check Out

Desired Data
☑ Desired Table Data
☑ Participant Data

Data Transfer Method
○ Dial Up
○ Diskette

* This screen can only b
data to or from the Loc

Forms

Clinic 07 (SEQ_ID - 46) has been loaded on the laptop.

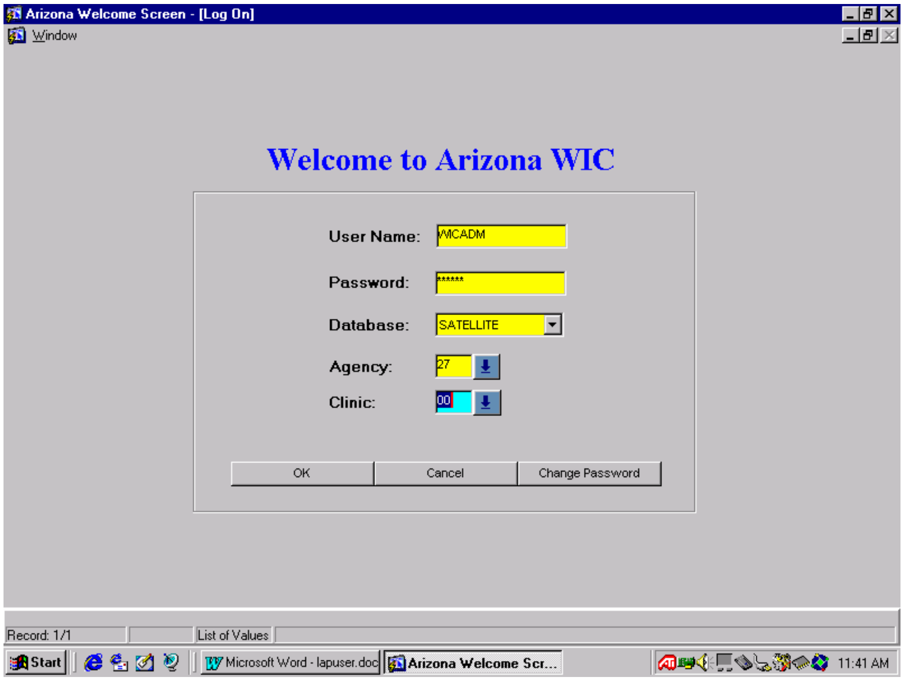
Select the Clinic from the list of values.
Record: 1/1

Figure 20 - Error Message

NOTE: Always check once a download has completed that you can log into AIM as the Clinic you plan on taking the laptop to. It is so much better than getting to Satellite only to find out there’s a problem you didn’t know about.

Unloading a Clinic from a Satellite Server Laptop to the Local Agency Server

1. If the laptop is not in the docking station, make sure the laptop is off and then load the laptop into the docking station. Start the laptop by pushing the “power on” button on the right hand side of the docking station.
2. Log into Windows with your designated Username and password. If your Windows logon screen has a domain LOV, select the LOV for your Local Agency. This will update the AIM software to the current version. When the update is complete and the black box goes away, log off.
3. Log into Windows with the Username “administrator” and no password. If your Windows logon screen has a domain LOV, select the domain which corresponds to your orange “PROPERTY OF ARIZONA DEPARTMENT OF HEALTH SERVICES” tag number.
4. Double-click on the “Load-Unload Clinic.reg” icon.
5. Start the AIM system.
6. Using your own AIM Username and password, log into the SATELLITE database, choose your Local Agency and you MUST select ‘00’ for all Clinics in order to perform the Unload Laptop functionality.



Welcome to Arizona WIC

User Name: WICADM

Password: ******

Database: SATELLITE

Agency: 27

Clinic: 00

Figure 21 - Login Screen

7. Click on “System Administration” on the AIM Main Menu.
8. From the System Administration dropdown menu, choose Notebook Admin. and then Load/Unload Laptop.

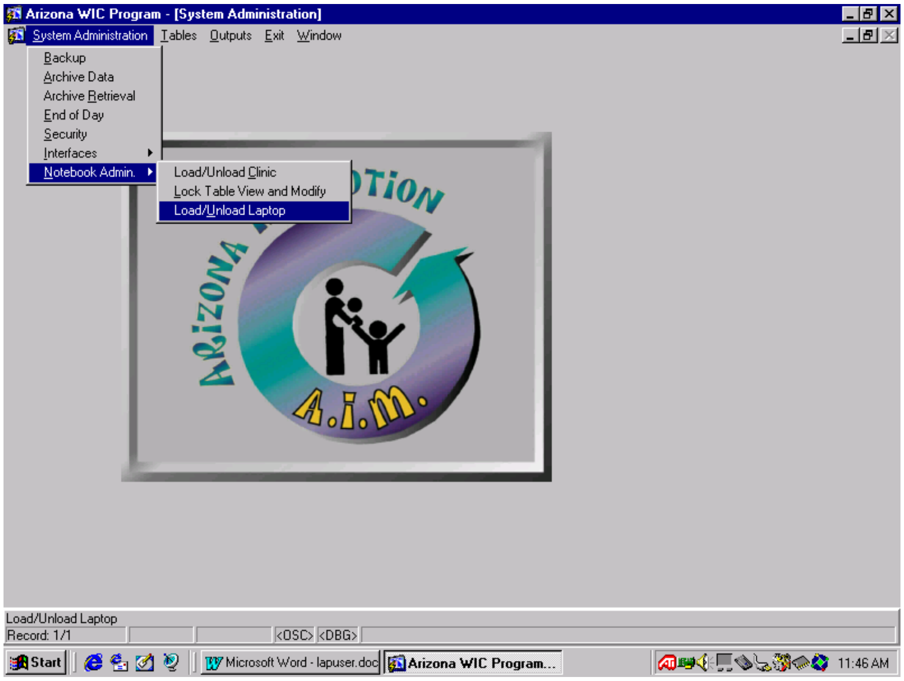
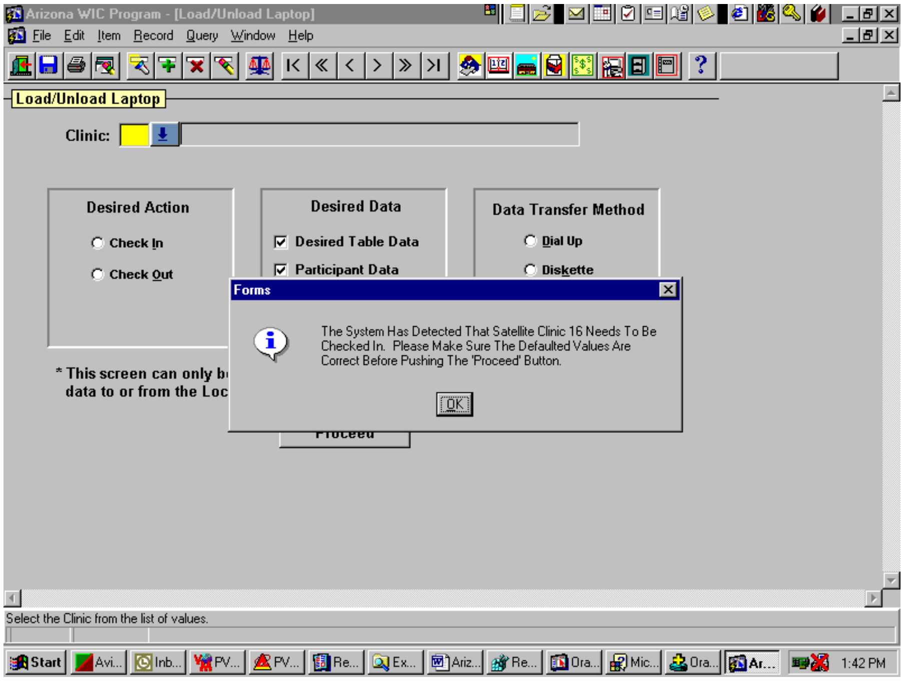


Figure 22 - Menu Path to Load/Unload Laptop

The software will check to see if a Clinic has been checked out. If one has, the following message will appear. Click OK. All the information should default in the proper fields.



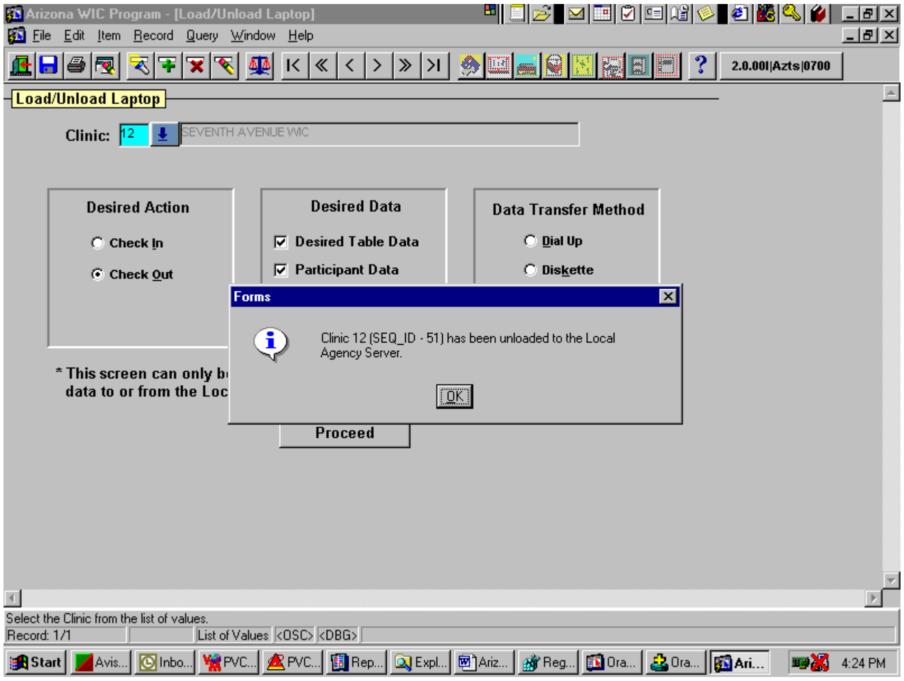
The System Has Detected That Satellite Clinic 16 Needs To Be Checked In. Please Make Sure The Defaulted Values Are Correct Before Pushing The 'Proceed' Button.

Select the Clinic from the list of values.

Figure 23 - Error Message

If the information does not default, choose the Clinic you wish to unload from the LOV or type in the Clinic code (if you know it) and press <TAB.

Desired Action: Check In.
Desired Data: Table Data and Participant Data. This is the default and should never be changed.
Data Transfer Method: Network. This is the default and currently the only functionality enabled in the AIM system.



Load/Unload Laptop

Clinic: 12 SEVENTH AVENUE WIC

Desired Action
○ Check In
● Check Out

Desired Data
☑ Desired Table Data
☑ Participant Data

Data Transfer Method
○ Dial Up
○ Diskette

* This screen can only b
data to or from the Loc

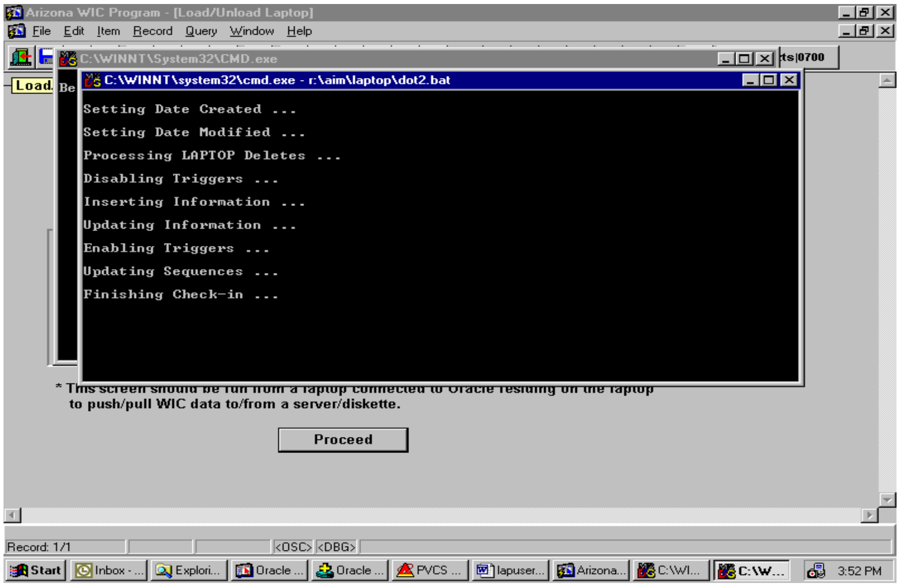
Forms
Clinic 12 (SEQ_ID - 51) has been unloaded to the Local Agency Server.

Select the Clinic from the list of values.
Record: 1/1

Figure 24 - Error Message

Press the “Proceed” button. The system will display a series of black boxes which will show the User that the process is running. The process should take no longer than 20 minutes.

Below is a picture of what the screen will look like while the Clinic is being unloaded from the laptop server to the Local Agency Server. Messages will be displayed to indicate the process' progress.

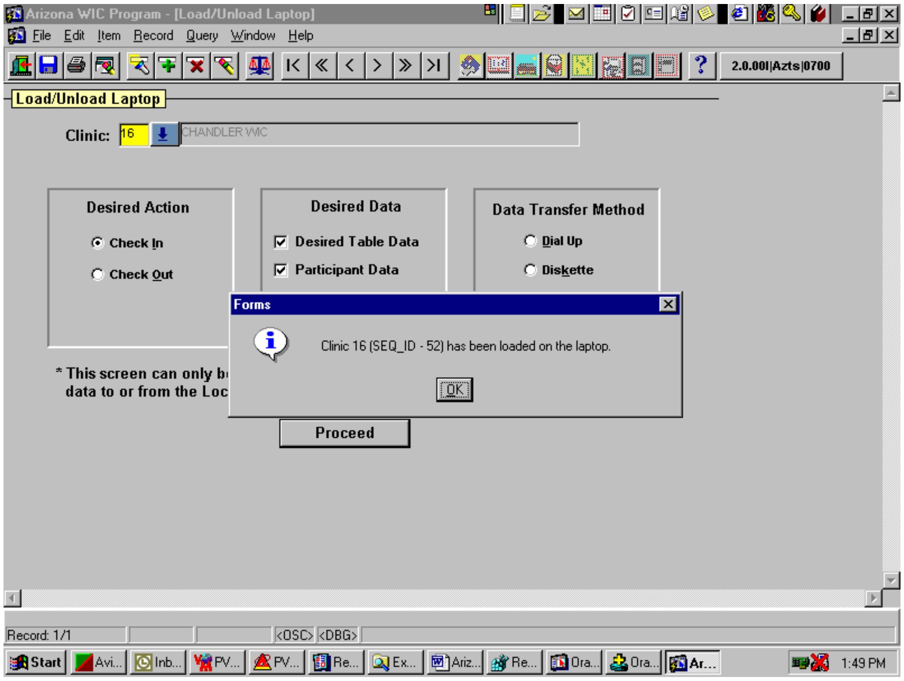

Arizona WIC Program - [Load/Unload Laptop]
File Edit Item Record Query Window Help
C:\WINNT\System32\CMD.exe
C:\WINNT\system32\cmd.exe - r:\aim\laptop\dot2.bat
Load
Be
ts|0700
Proceed
Record: 1/1
<OSC> <DBG>
Start
Inbox - ...
Explori...
Oracle ...
Oracle ...
PVCS ...
lapuser...
Arizona...
C:\WI...
C:\W...
3:52 PM

```
Setting Date Created ...
Setting Date Modified ...
Processing LAPTOP Deletes ...
Disabling Triggers ...
Inserting Information ...
Updating Information ...
Enabling Triggers ...
Updating Sequences ...
Finishing Check-in ...
```

* This screen should be run from a laptop connected to Oracle residing on the laptop to push/pull WIC data to/from a server/diskette.

Figure 25 - MS/DOS Windows

The following message will appear when the laptop unload has successfully completed.


Arizona WIC Program - [Load/Unload Laptop]
File Edit Item Record Query Window Help
2.0.001|Azts|0700
Proceed
OK
Record: 1/1
<OSC> <DBG>
Start
1:49 PM

Load/Unload Laptop

Clinic: 16 CHANDLER WIC

Desired Action
● Check In
○ Check Out

Desired Data
☑ Desired Table Data
☑ Participant Data

Data Transfer Method
○ Dial Up
○ Diskette

* This screen can only b
data to or from the Loc

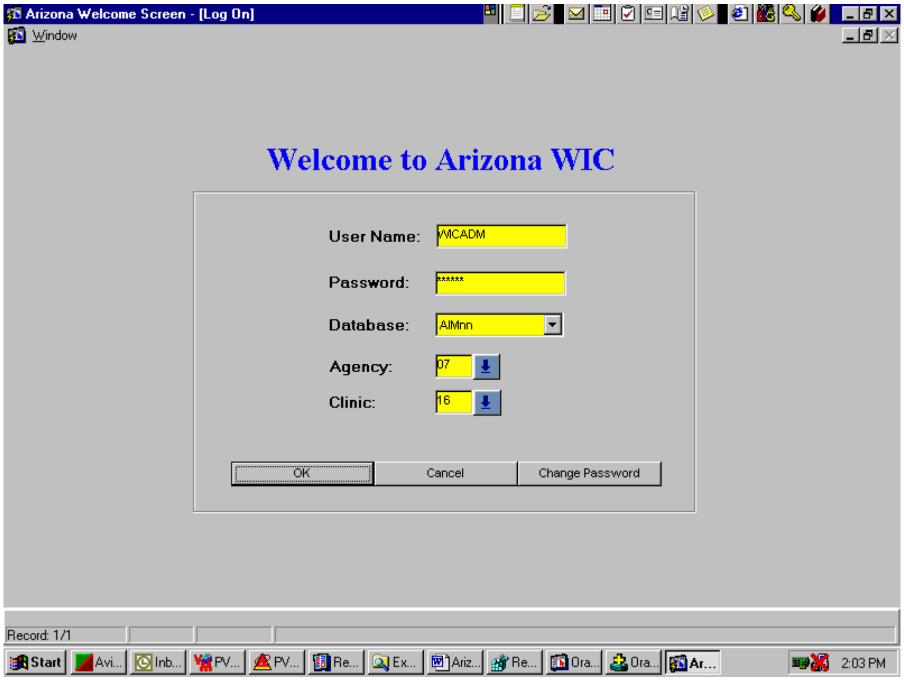
Forms

Clinic 16 (SEQ_ID - 52) has been loaded on the laptop.

Figure 26 - Laptop Unload Success Message

Using a Server or Client Laptop at a Permanent Clinic Using the Local Agency Server.

1. If the laptop is not in the docking station, make sure the laptop is off and then load the laptop into the docking station. Start the laptop by pushing the “power on” button on the right hand side of the docking station.
2. Log into Windows with your designated Username and password. If your Windows logon screen has a domain LOV, select the LOV for your Local Agency. This will update the AIM software to the current version.
3. Double-click on the “Docking Station.reg” icon.
4. Start the AIM system.
5. Using your own AIM Username and password, select AIMnn from the Database LOV, where nn = your Local Agency number.
6. You are now ready to do an FI Test Print and see clients.



User Name: WICADM

Password: ******

Database: AIMnn

Agency: 07

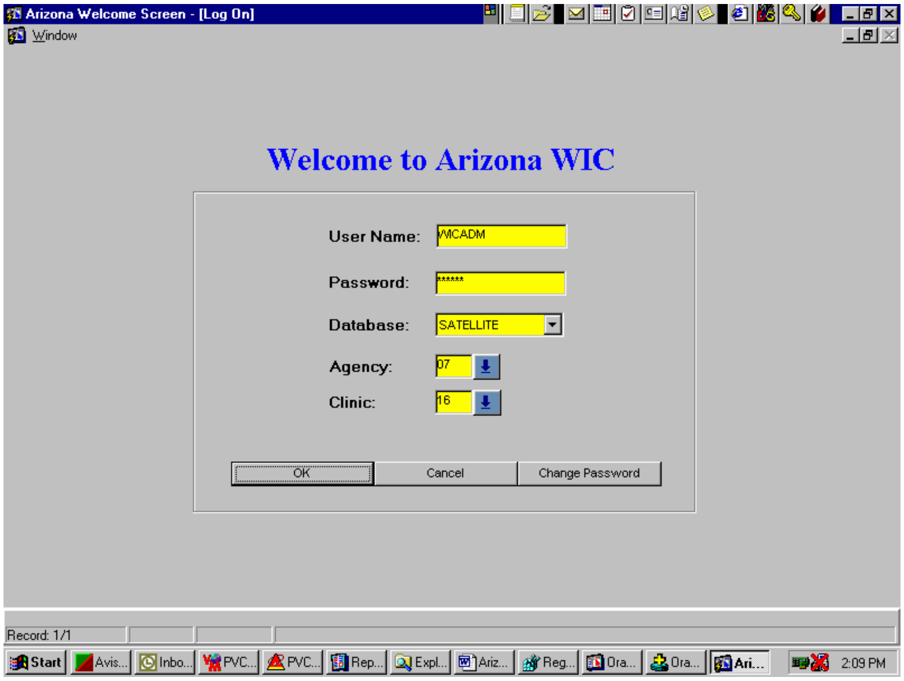
Clinic: 16

Figure 27 - Login Screen

Using a Server or Client Laptop at a Satellite Clinic

1. Start the laptop by pushing the “power on” button to the right.
2. Log into Windows with Username “administrator” and no password. If your Windows logon screen has a domain LOV, select the LOV which corresponds to the orange “PROPERTY OF ARIZONA DEPARTMENT OF HEALTH SERVICES” tag number on the laptop.
3. On a ***SERVER*** laptop, double-click on the “nnnnn Server.reg” icon where nnnnn corresponds to the number on the orange “PROPERTY OF ARIZONA DEPARTMENT OF HEALTH SERVICES” tag on the ***SERVER*** laptop.
4. On a ***CLIENT*** laptop, double-click on the “nnnnn Server.reg” icon where nnnnn corresponds to the number on the orange “PROPERTY OF ARIZONA DEPARTMENT OF HEALTH SERVICES” tag on the ***SERVER*** laptop.
5. Start the AIM system.
6. Using your own AIM Username and password, select SATELLITE from the Database LOV,
7. You are now ready to do an FI Test Print and see clients.

NOTE: If you are running with a server laptop and client laptop(s), do an FI Test Print on each one.



User Name: WICADM

Password: ******

Database: SATELLITE

Agency: 07

Clinic: 16

Figure 28 - Login Screen

Troubleshooting Tips & Tricks

MICR Fonts

LexMark Printers

1. If the MICR font is not printing on a LexMark printer, you have forgotten to double-click on the “nnnnn Server.reg” icon (if you’re at a satellite) or you have not double_clicked the “Docking Station.reg” icon if you’re trying to see clients at a permanent Clinic attached to the Local Agency server.
2. If the MICR font is still not printing correctly, call the AIM Help Desk.

HP1100 Printers

1. If the MICR font does not print correctly on theFI Test Print, minimize AIM, double-click the “nnnnn Server.reg” icon on the laptop, maximize AIM and try the FI Test Print again.
2. If the MICR font prints still does not print correctly, click on the Start button, then select Settings, Printers.

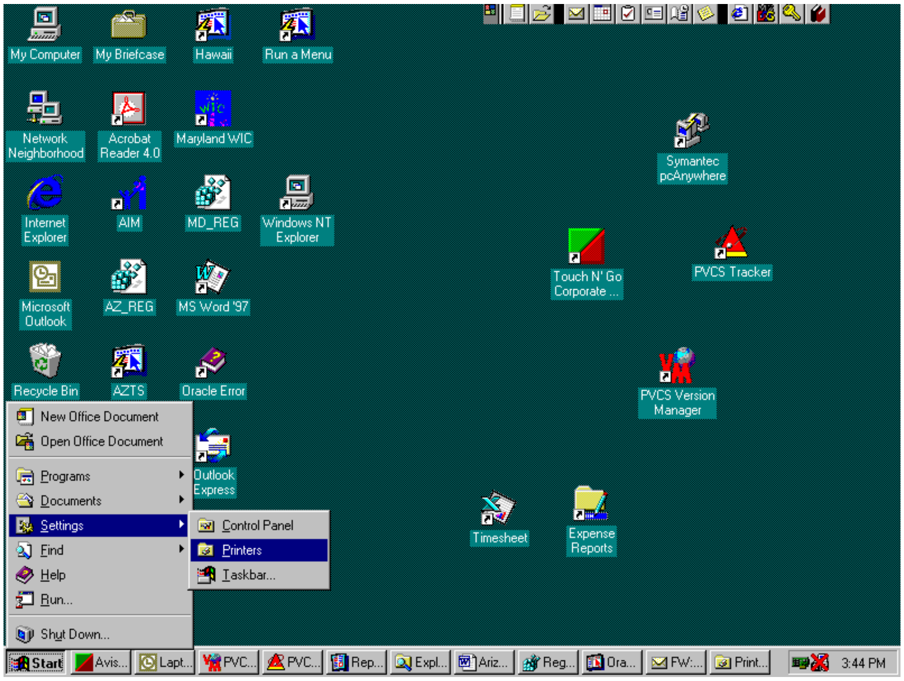


Figure 29 - Navigation Path to Printer Settings

3. Double-click on AZ Check Laptop Printer. Click on Printer, then Properties.

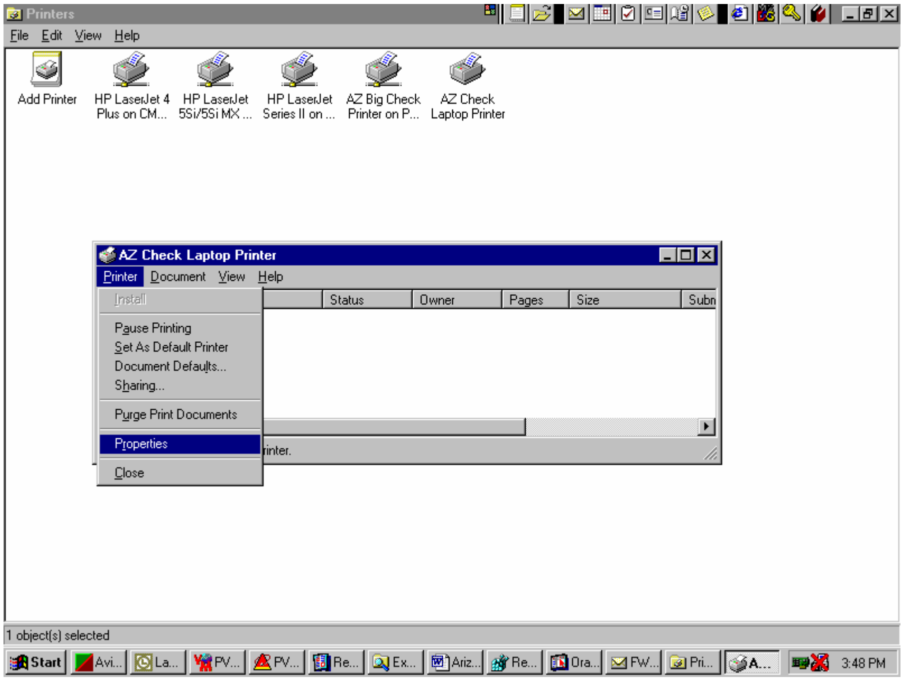
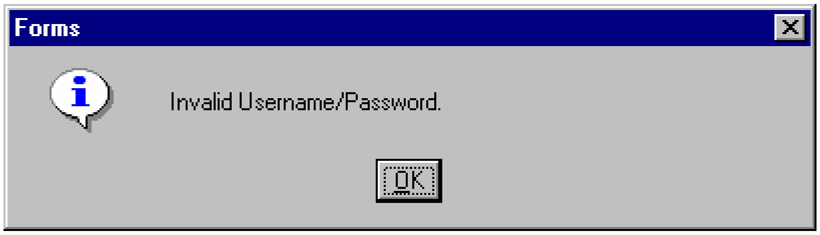


Figure 30 - Menu Path to Printer Properties

4. Click on the User Customize tab at the top right., Click on Download Font.
5. Click on the Search Path button and close the printer box which comes up again.
6. In the Available Fonts window, you should see “E-13B MICR Uk [8.0 Pt.] (100). If it is not highlighted (blue in color), click on it.
7. Click on the Download button and close all windows. Re-try the FI Test Print.
8. If the MICR line, still does not print correctly, call the AIM Help Desk.

"Empty" Laptops

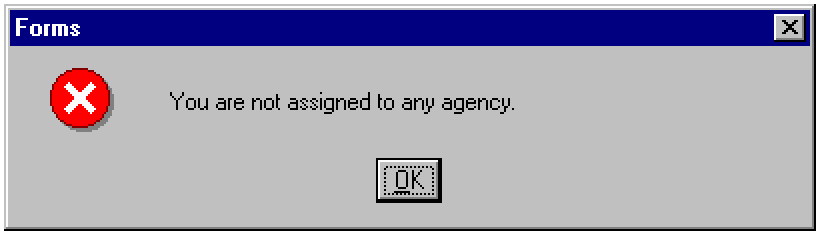
Occasionally, the network lines will "hiccup", if you will, causing the laptop process to fail in the middle. If, after having done a download, you have either of the following problems occur:



Invalid Username/Password.

Figure 31 - Error Message

OR



You are not assigned to any agency.

Figure 32 - Error Message

1. Close the AIM application and click on the Start button and select Programs, Windows NT Explorer.

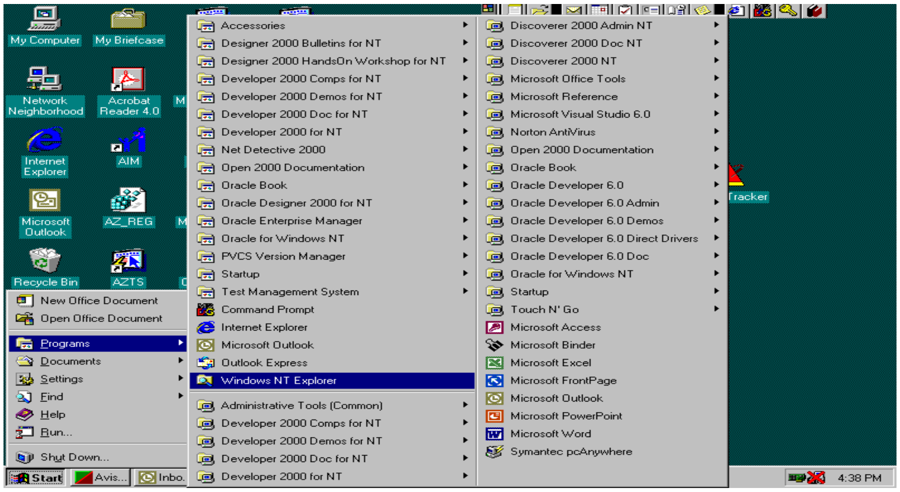
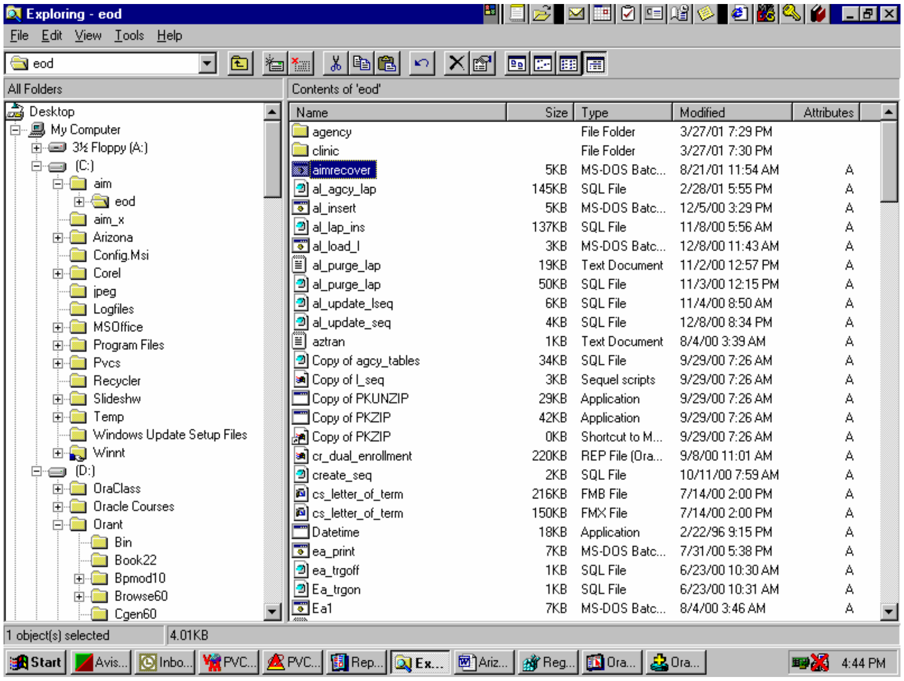


Figure 33 - Path to Windows Explorer

2. Click on the plus sign (+) to the left of the aim folder and then click on the yellow folder next

to the word eod.

3. In the window on the right-hand side of the screen, you should see a file called aimrecover or aimrecover.bat. Double-click on the blue and white box to the left of the word aimrecover.



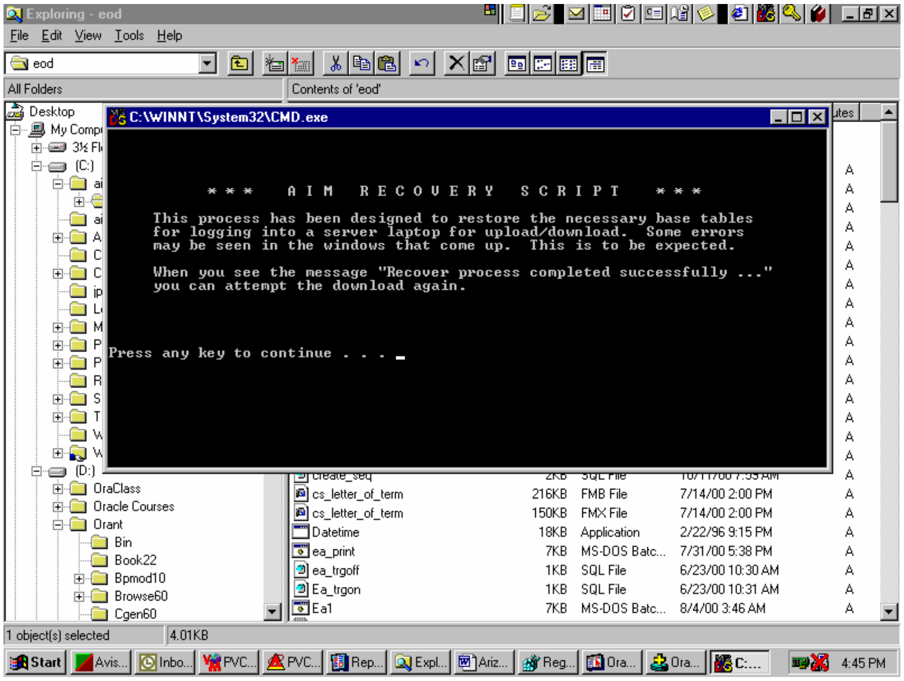
Contents of 'eod'

Name	Size	Type	Modified	Attributes
agency		File Folder	3/27/01 7:29 PM	
clinic		File Folder	3/27/01 7:30 PM	
aimrecover	5KB	MS-DOS Batc...	8/21/01 11:54 AM	A
al_agcy_lap	145KB	SQL File	2/28/01 5:55 PM	A
al_insert	5KB	MS-DOS Batc...	12/5/00 3:29 PM	A
al_lap_ins	137KB	SQL File	11/8/00 5:56 AM	A
al_load_l	3KB	MS-DOS Batc...	12/8/00 11:43 AM	A
al_purge_lap	19KB	Text Document	11/2/00 12:57 PM	A
al_purge_lap	50KB	SQL File	11/3/00 12:15 PM	A
al_update_lseq	6KB	SQL File	11/4/00 8:50 AM	A
al_update_seq	4KB	SQL File	12/8/00 8:34 PM	A
aztran	1KB	Text Document	8/4/00 3:39 AM	A
Copy of agcy_tables	34KB	SQL File	9/29/00 7:26 AM	A
Copy of l_seq	3KB	Sequel scripts	9/29/00 7:26 AM	A
Copy of PKUNZIP	29KB	Application	9/29/00 7:26 AM	A
Copy of PKZIP	42KB	Application	9/29/00 7:26 AM	A
Copy of PKZIP	0KB	Shortcut to M...	9/29/00 7:26 AM	A
cr_dual_enrollment	220KB	REP File (Ora...	9/8/00 11:01 AM	A
create_seq	2KB	SQL File	10/11/00 7:59 AM	A
cs_letter_of_term	216KB	FMB File	7/14/00 2:00 PM	A
cs_letter_of_term	150KB	FMX File	7/14/00 2:00 PM	A
Datetime	18KB	Application	2/22/96 9:15 PM	A
ea_print	7KB	MS-DOS Batc...	7/31/00 5:38 PM	A
ea_trgoff	1KB	SQL File	6/23/00 10:30 AM	A
Ea_trgon	1KB	SQL File	6/23/00 10:31 AM	A
Ea1	7KB	MS-DOS Batc...	8/4/00 3:46 AM	A

1 object(s) selected 4.01KB

Figure 34 - Directory Location of "Aimrecover"

This is the screen you will see. Follow the instructions. This process takes no longer than ten (10) minutes to complete and restores the necessary base tables minimally required to get logged in to AIM and try the download again.



```
          * * *   A I M   R E C O V E R Y   S C R I P T   * * *

     This process has been designed to restore the necessary base tables
     for logging into a server laptop for upload/download.  Some errors
     may be seen in the windows that come up.  This is to be expected.

     When you see the message "Recover process completed successfully ..."
     you can attempt the download again.



Press any key to continue . . . _
```

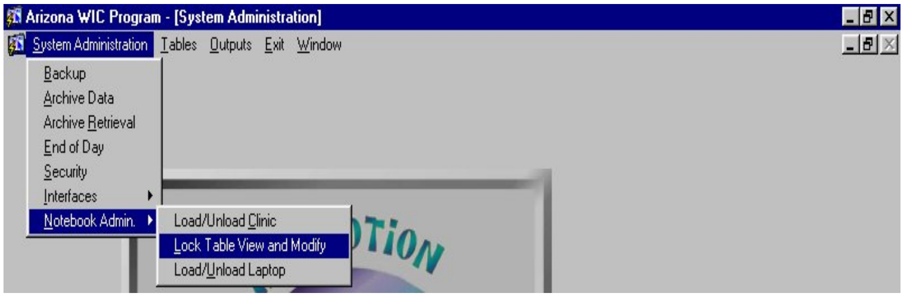
cs_letter_of_term	216KB	FMB File	7/14/00 2:00 PM	A
cs_letter_of_term	150KB	FMX File	7/14/00 2:00 PM	A
Datetime	18KB	Application	2/22/96 9:15 PM	A
ea_print	7KB	MS-DOS Batc...	7/31/00 5:38 PM	A
ea_trgoff	1KB	SQL File	6/23/00 10:30 AM	A
Ea_trgon	1KB	SQL File	6/23/00 10:31 AM	A
Ea1	7KB	MS-DOS Batc...	8/4/00 3:46 AM	A

Figure 35 - “Aimrecover at Work” Window

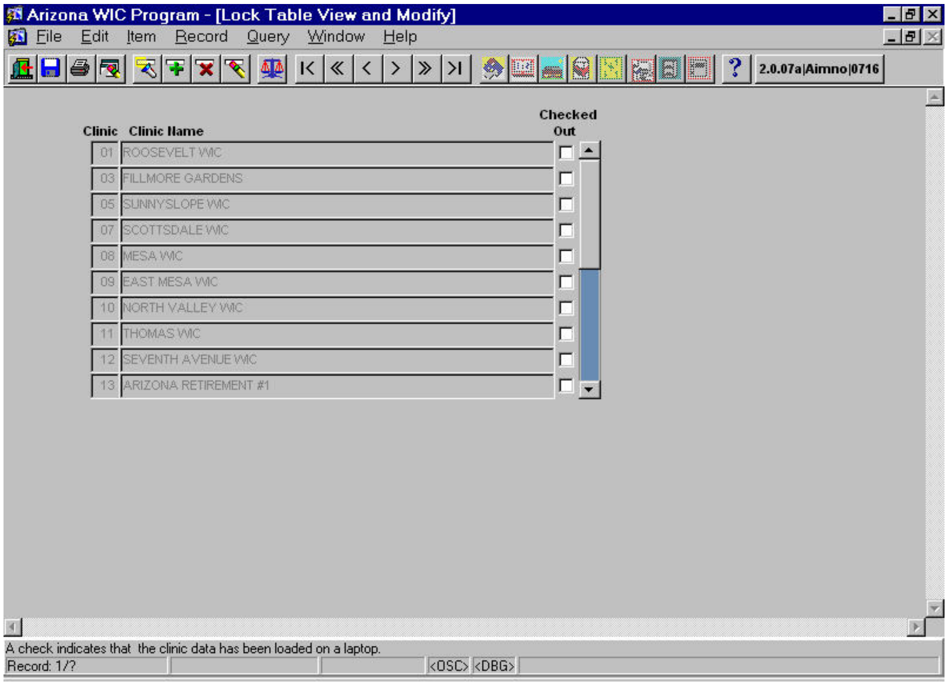
Locking Table View and Modifying

To Lock Table View and Modify:

1. Click on System Administration from the menu bar.
2. Position the cursor on Notebook Adm, the sub-menu is displayed.
3. Click on Lock Table View and Modify as shown below:



The Lock Table and Modify Window is displayed:



Clinic	Clinic Name	Checked Out
01	ROOSEVELT WIC	□
03	FILLMORE GARDENS	□
05	SUNNYSLOPE WIC	□
07	SCOTTSDALE WIC	□
08	MESA WIC	□
09	EAST MESA WIC	□
10	NORTH VALLEY WIC	□
11	THOMAS WIC	□
12	SEVENTH AVENUE WIC	□
13	ARIZONA RETIREMENT #1	□

A check indicates that the clinic data has been loaded on a laptop.
Record: 1/? <OSC> <DBG>

Figure 36 - Lock Table View & Modify

View Clinics Currently Loaded onto Remote Clinic Servers

1. Press the F8 key and the system will display a list of all the WIC/CSFP Clinics and their corresponding Clinic ID numbers.
2. Click on the down arrow of the scroll bar to the right of the Checked Out field to view Clinics that are not displayed on the screen.
3. A check mark in the Check Out field next to a Clinic Name record indicates that the Clinic data has been loaded onto a laptop.

Modify Clinics Currently Loaded onto Remote Clinic Servers

1. In the situation where a Clinic was checked out in error, rather than loading the Clinic back onto the Local Agency server, you may simply uncheck the Checked Out Box.

Warning: This step must only be performed when no changes have been Made to the Clinic data on the remote Clinic servers. Otherwise, no data changes will be saved to the Local Agency server.

2. Click on the Exit icon to exit the screen.

Fields

Clinic - The ID number of the Clinic. This field is display only.
Clinic Name - The name of the Clinic associated with the Clinic field. This field is display only.

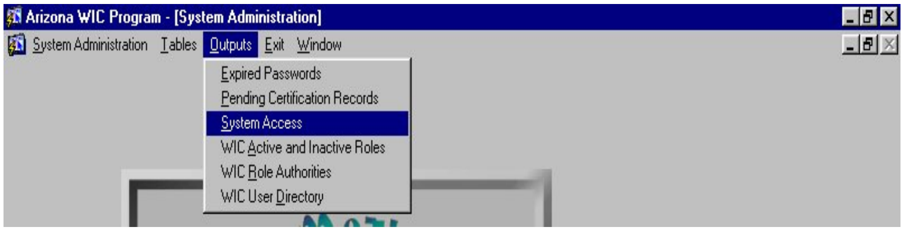
Check Box

Check Out - Check mark indicates the Clinic is checked out to remote Clinic server.

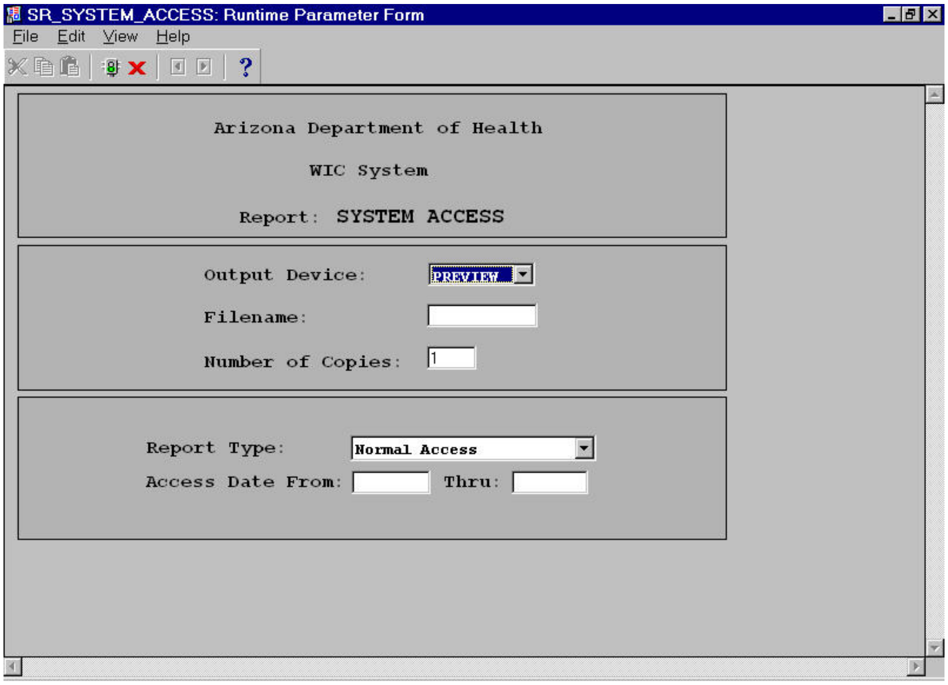
Producing a System Access Report

To Produce a System Access Report:

1. Click on Outputs from the menu bar.
2. Click on System Access as shown below:



The System Access Window is displayed:



Arizona Department of Health

WIC System

Report: SYSTEM ACCESS

Output Device: PREVIEW

Filename:

Number of Copies: 1

Report Type: Normal Access

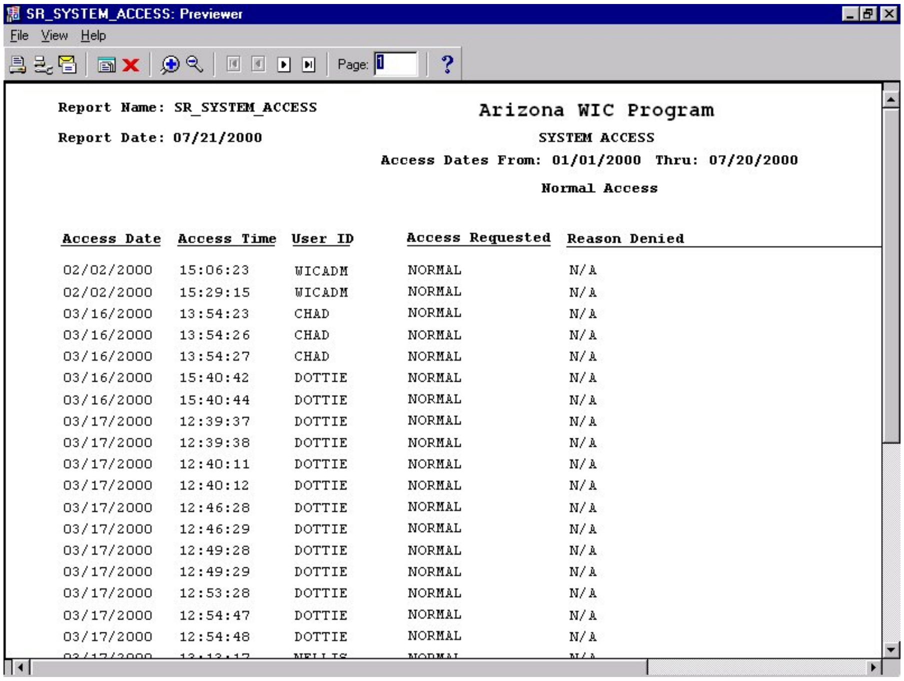
Access Date From: Thru:

Figure 37 - System Access Report

Produce a System Access Report

1. Click the down arrow in the Output Device field to activate the drop down box, then select which Output Device you want the System Access report sent to by double clicking on that device name.
2. TAB to the Filename field. Enter the filename to give to the report you are generating.
3. TAB to the Number of Copies field. Select the number of report copies desired by typing that number in this field.
4. Determine which of the following types of System Access report to view (Normal, Unauthorized, or Unusual) by clicking once on the appropriate list box.

5. Next, click the Access Date From field and enter the beginning access date to be covered. This date should be formatted MM/DD/YYYY.
6. Press the TAB key once to move to the Thru field and enter the ending access date you want the report to cover. This date should be formatted MM/DD/YYYY.
7. Click the green light icon to bring up the preview screen shown below:



```
Report Name: SR_SYSTEM_ACCESS                Arizona WIC Program
Report Date: 07/21/2000                         SYSTEM ACCESS
                                   Access Dates From: 01/01/2000  Thru: 07/20/2000
                                                Normal Access

Access Date  Access Time  User ID     Access Requested  Reason Denied

02/02/2000   15:06:23     WICADM      NORMAL            N/A
02/02/2000   15:29:15     WICADM      NORMAL            N/A
03/16/2000   13:54:23     CHAD        NORMAL            N/A
03/16/2000   13:54:26     CHAD        NORMAL            N/A
03/16/2000   13:54:27     CHAD        NORMAL            N/A
03/16/2000   15:40:42     DOTTIE      NORMAL            N/A
03/16/2000   15:40:44     DOTTIE      NORMAL            N/A
03/17/2000   12:39:37     DOTTIE      NORMAL            N/A
03/17/2000   12:39:38     DOTTIE      NORMAL            N/A
03/17/2000   12:40:11     DOTTIE      NORMAL            N/A
03/17/2000   12:40:12     DOTTIE      NORMAL            N/A
03/17/2000   12:46:28     DOTTIE      NORMAL            N/A
03/17/2000   12:46:29     DOTTIE      NORMAL            N/A
03/17/2000   12:49:28     DOTTIE      NORMAL            N/A
03/17/2000   12:49:29     DOTTIE      NORMAL            N/A
03/17/2000   12:53:28     DOTTIE      NORMAL            N/A
03/17/2000   12:54:47     DOTTIE      NORMAL            N/A
03/17/2000   12:54:48     DOTTIE      NORMAL            N/A
03/17/2000   13:13:17     NELLIS      NORMAL            N/A
```

Figure 38 - System Access Report Sample

Sample of a System Access Report

8. Click the Previous, Next, First, Last, and Page icons at the top of the screen to move forward and backward through the report pages.
9. Click the Close icon to exit the preview screen. Click the New icon to view a new copy of the same preview screen.

Fields

Output Device - The User may select (from a drop down list) PREVIEW, SCREEN, PRINTER, HTML, RTF or PDF.
File Name - If file is selected (above), the directory and filename are entered.
Number of Copies - If printer is selected (above), the number of copies desired is entered.
Report Type - A list box to give the User a choice of report types. (Normal, unauthorized, etc.)
Access Date From/Thru - The range of dates upon which the report will filter data, excluding information not falling within the specified range. These fields are mandatory.

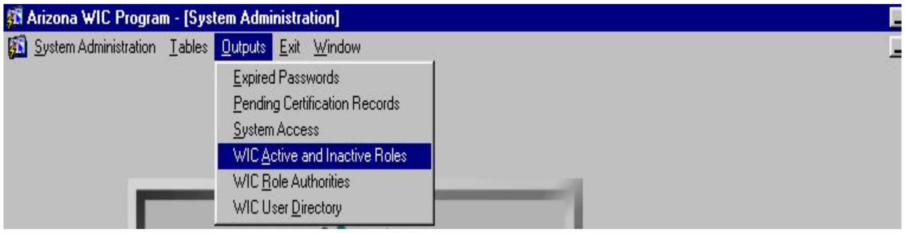
Calculations

None

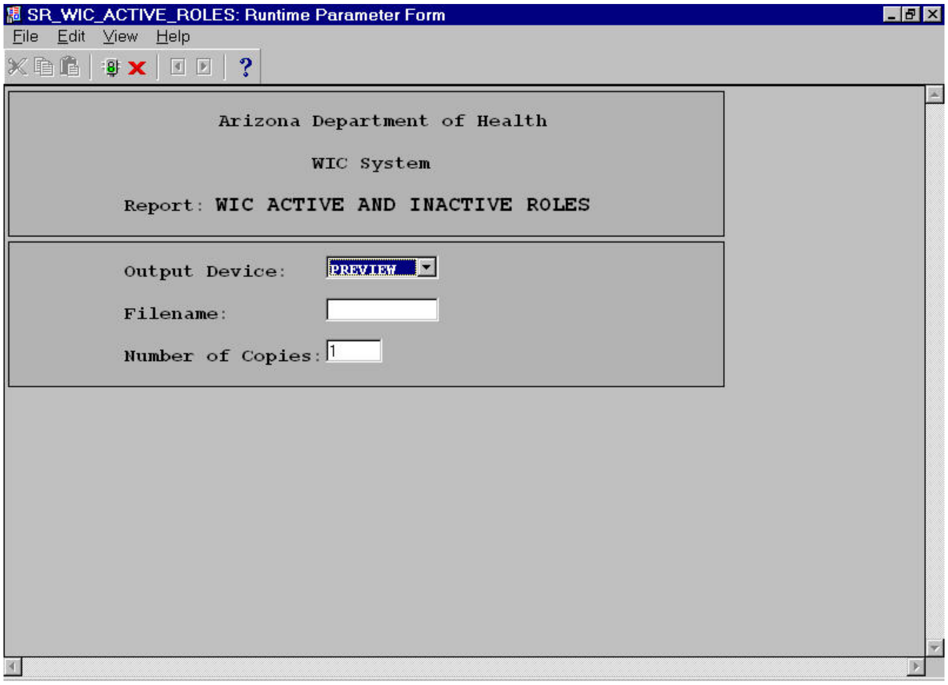
Producing a WIC Active and Inactive Roles Report

To Produce a WIC Active and Inactive Roles Report:

1. Click on Outputs from the menu bar.
2. Click on WIC Active and Inactive Roles as shown below:



The WIC Active and Inactive Roles Window is displayed:



Arizona Department of Health

WIC System

Report: WIC ACTIVE AND INACTIVE ROLES

Output Device: PREVIEW

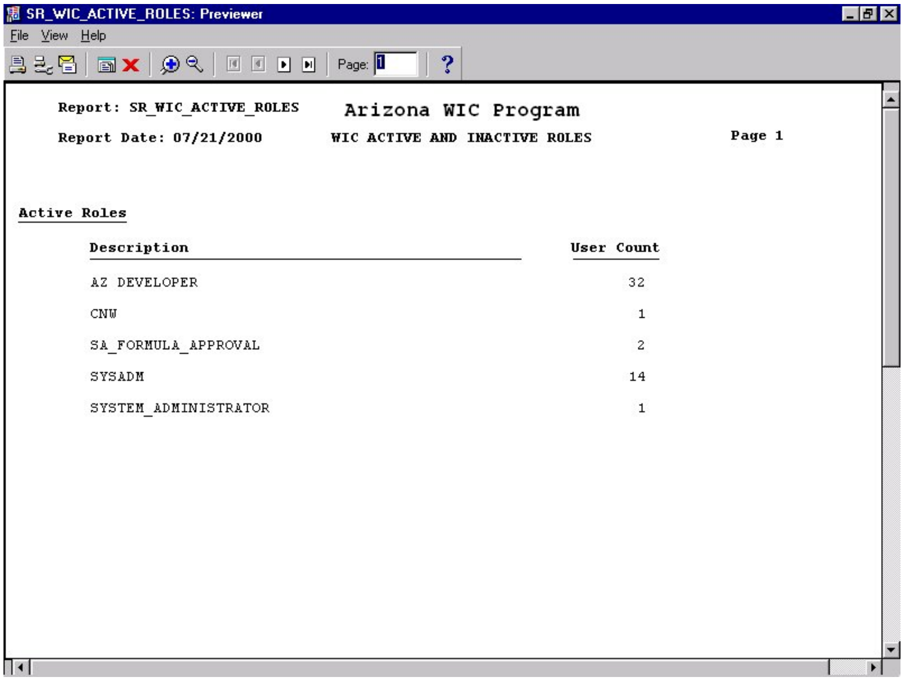
Filename:

Number of Copies: 1

Figure 39 - WIC Active & Inactive Roles

Produce a WIC Active and Inactive Roles Report

1. Click the down arrow in the Output Device field to activate the drop down box, then select which Output Device to send the WIC Active and Inactive Roles report to by double clicking on that device name.
2. TAB to the Filename field. Enter the filename to give the report you are generating.
3. TAB to the Number of Copies field. Select the number of report copies by typing that number in this field.
4. Click the green light icon to bring up the preview screen shown below:



```
Report: SR_WIC_ACTIVE_ROLES     Arizona WIC Program
Report Date: 07/21/2000         WIC ACTIVE AND INACTIVE ROLES          Page 1

Active Roles

    Description                                          User Count

    AZ DEVELOPER                                                32
    CNW                                                          1
    SA_FORMULA_APPROVAL                                          2
    SYSADM                                                      14
    SYSTEM_ADMINISTRATOR                                         1
```

Figure 40 - WIC Active & Inactive Roles Sample

Sample WIC Active and Inactive Roles Report

5. Click the Previous, Next, First, Last, and Page icons at the top of the screen to move forward and backward through the report pages.
6. Click the Close icon to exit the preview screen. Click the New icon to view a new copy of the same preview screen.

Fields

Output Device - The User may select (from a drop down list) PREVIEW, SCREEN, PRINTER, HTML, RTF or PDF.
File Name - If file is selected (above), the directory and filename are entered.
Number of Copies - If printer is selected (above), the number of copies desired is entered.

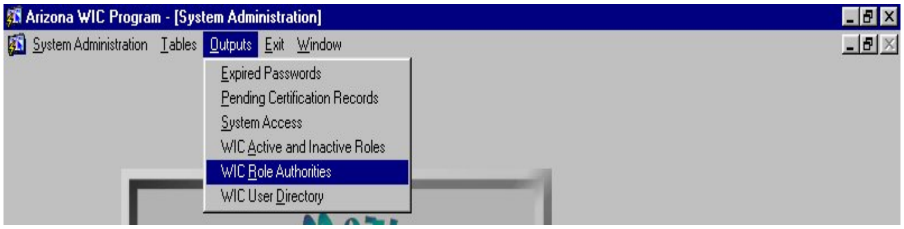
Calculations

User Count – A count of Users in a Local Agency/Clinic with an active role.

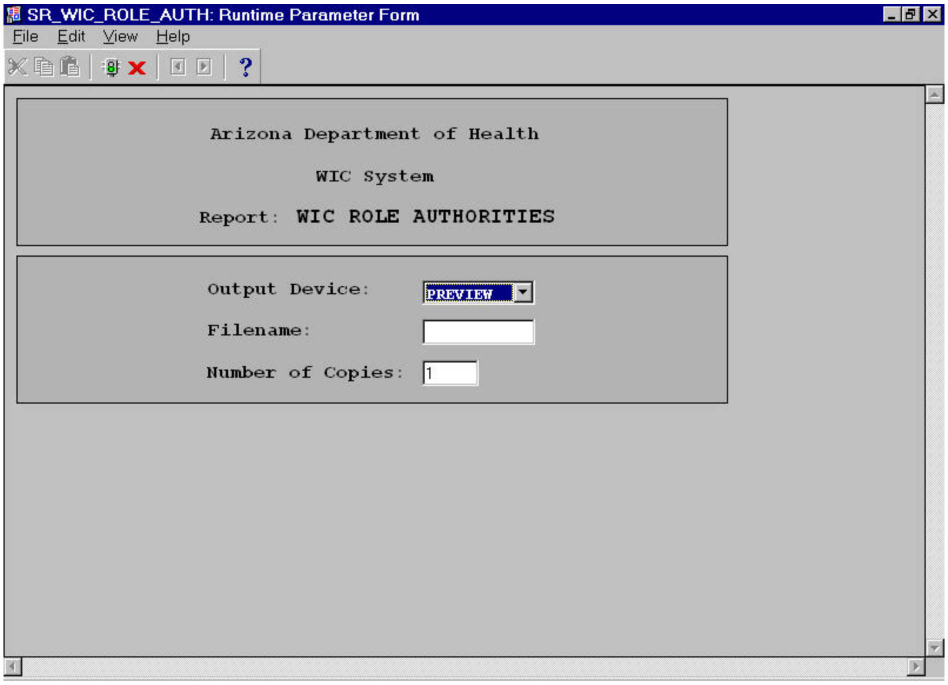
Producing a WIC Role Authorities Report

To Produce a WIC Role Authorities Report:

1. Click on Outputs from the menu bar.
2. Click on WIC Role Authorities as shown below:



The WIC Roles Authorities Window is displayed:



Arizona Department of Health

WIC System

Report: WIC ROLE AUTHORITIES

Output Device: PREVIEW

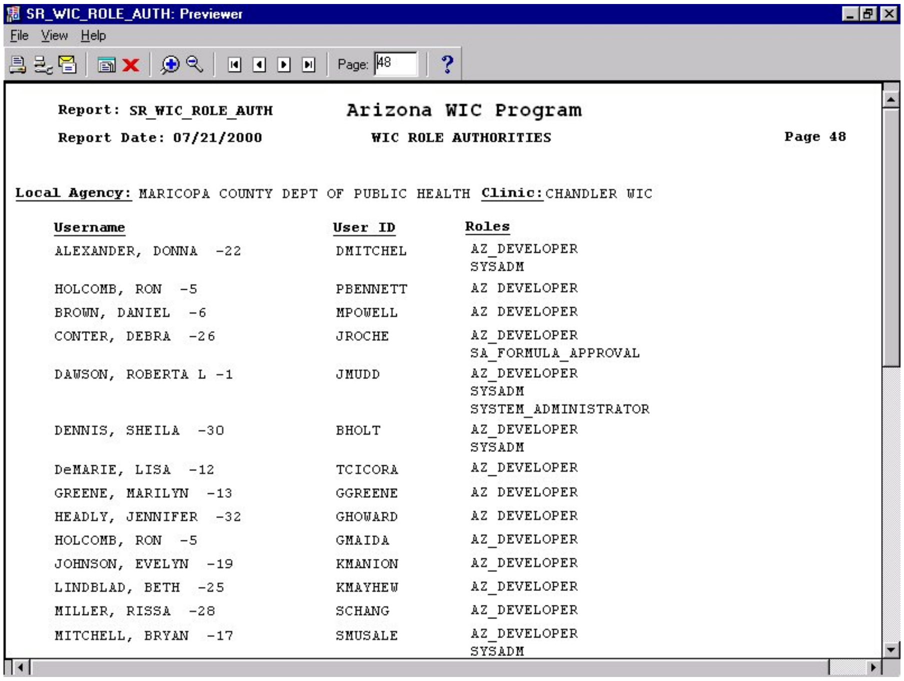
Filename:

Number of Copies: 1

Figure 41 - WIC Role Authorities

Produce a WIC Role Authorities Report

1. Click the down arrow in the Output Device field to activate the drop down box, then select which Output Device to send the WIC Role Authorities report to by double clicking on that device name.
2. TAB to the Filename field. Enter the filename to give to the report generating.
3. TAB to the Number of Copies field. Select the number of report copies by typing that number in this field.
4. Click the green light icon to bring up the preview screen shown below:



```
     Report: SR_WIC_ROLE_AUTH          Arizona WIC Program
     Report Date: 07/21/2000             WIC ROLE AUTHORITIES                            Page 48

Local Agency: MARICOPA COUNTY DEPT OF PUBLIC HEALTH Clinic:CHANDLER WIC

    Username                       User ID        Roles
    ALEXANDER, DONNA  -22          DMITCHEL        AZ_DEVELOPER
                                                   SYSADM
    HOLCOMB, RON  -5               PBENNETT        AZ DEVELOPER
    BROWN, DANIEL  -6              MPOWELL         AZ DEVELOPER
    CONTER, DEBRA  -26             JROCHE          AZ_DEVELOPER
                                                   SA_FORMULA_APPROVAL
    DAWSON, ROBERTA L -1           JMUDD           AZ_DEVELOPER
                                                   SYSADM
                                                   SYSTEM_ADMINISTRATOR
    DENNIS, SHEILA  -30            BHOLT           AZ_DEVELOPER
                                                   SYSADM
    DeMARIE, LISA  -12             TCICORA         AZ_DEVELOPER
    GREENE, MARILYN  -13           GGREENE         AZ DEVELOPER
    HEADLY, JENNIFER  -32          GHOWARD         AZ DEVELOPER
    HOLCOMB, RON  -5               GMAIDA          AZ_DEVELOPER
    JOHNSON, EVELYN  -19           KMANION         AZ_DEVELOPER
    LINDBLAD, BETH  -25            KMAYHEW         AZ_DEVELOPER
    MILLER, RISSA  -28             SCHANG          AZ_DEVELOPER
    MITCHELL, BRYAN  -17           SMUSALE         AZ_DEVELOPER
                                                   SYSADM
```

Figure 42 - WIC Role Authorities Sample

Sample WIC Role Authorities Report

5. Click the Previous, Next, First, Last, and Page icons at the top of the screen to move forward and backward through the report pages.
6. Click the Close icon to exit the preview screen. Click the New icon to view a new copy of the same preview screen.

Fields

Output Device - The User may select (from a drop down list) PREVIEW, SCREEN, PRINTER, HTML, RTF or PDF.
File Name - If file is selected (above), the directory and filename are entered.
Number of Copies - If printer is selected (above), the number of copies desired is entered.

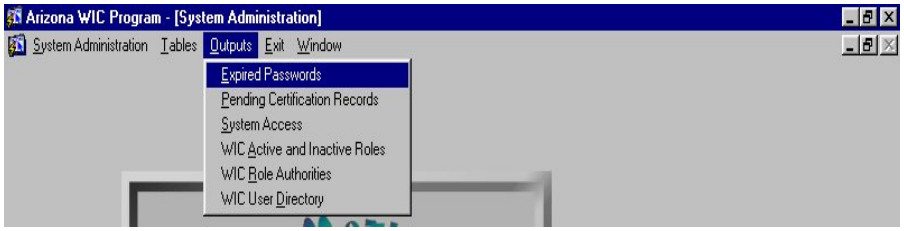
Calculations

None

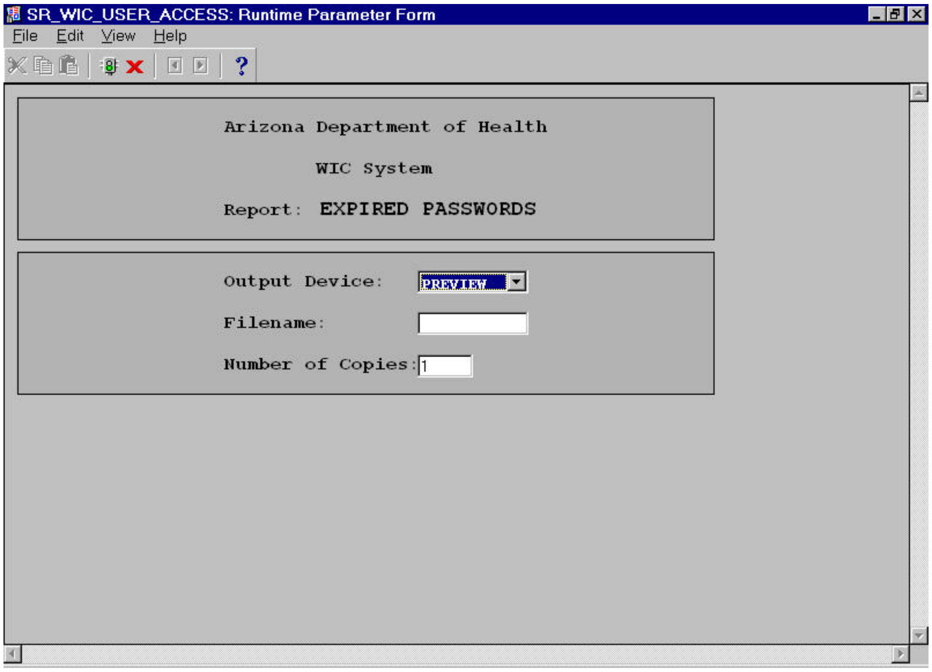
Producing an Expired Passwords Report

To Produce an Expired Passwords Report:

1. Click on Outputs from the menu bar.
2. Click on Expired Passwords as shown below:



The WIC User Access Window is displayed:



Arizona Department of Health

WIC System

Report: EXPIRED PASSWORDS

Output Device: PREVIEW

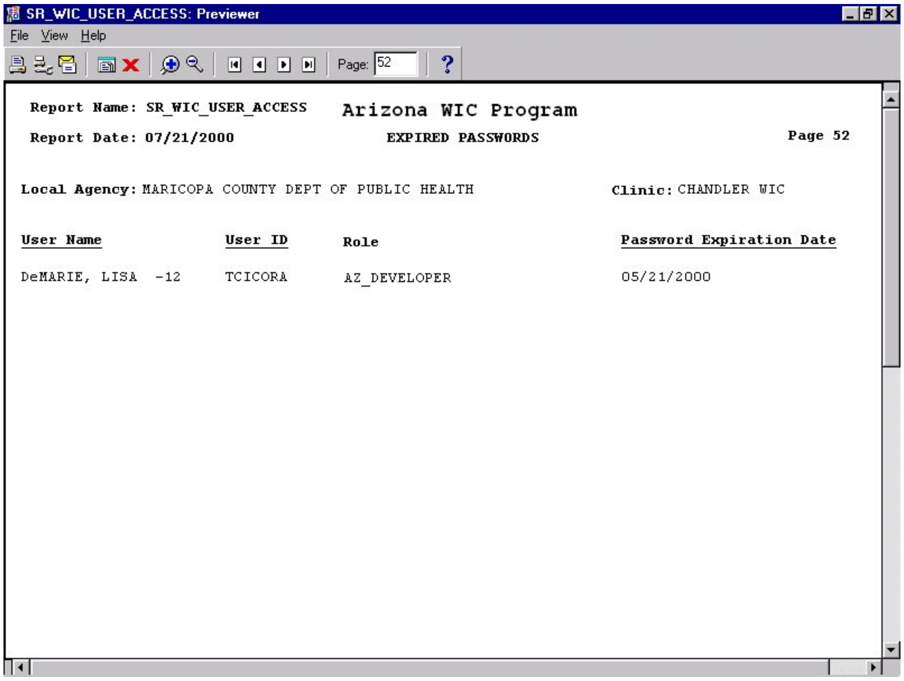
Filename:

Number of Copies: 1

Figure 43 - Expired Passwords Report

Produce an Expired Passwords Report

1. Click the down arrow in the Output Device field to activate the drop down box, then select which Output Device to send the WIC User Access report to by double clicking on that device name.
2. TAB to the Filename field. Enter the filename the report being generated is to be called.
3. TAB to the Number of Copies field. Select the number of report copies desired by typing that number in this field.
4. Click the green light icon to bring up the preview screen shown below:



```
Report Name: SR_WIC_USER_ACCESS    Arizona WIC Program
Report Date: 07/21/2000                EXPIRED PASSWORDS                    Page 52

Local Agency: MARICOPA COUNTY DEPT OF PUBLIC HEALTH            Clinic: CHANDLER WIC

User Name            User ID      Role                            Password Expiration Date

DeMARIE, LISA  -12   TCICORA      AZ_DEVELOPER                    05/21/2000
```

Figure 44 - Expired Passwords Report Sample

Sample WIC User Access Report

5. Click the Previous, Next, First, Last, and Page icons at the top of the screen to move forward and backward through the report pages.
6. Click the Close icon to exit the preview screen. Click the New icon to view a new copy of the same preview screen.

Fields

Output Device - The User may select (from a drop down list) PREVIEW, SCREEN, PRINTER, HTML, RTF or PDF.
File Name - If file is selected (above), the directory and filename are entered.
Number of Copies - If printer is selected (above), the number of copies desired is entered.

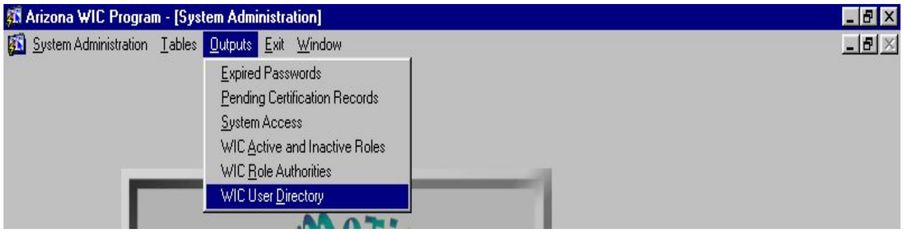
Calculations

None

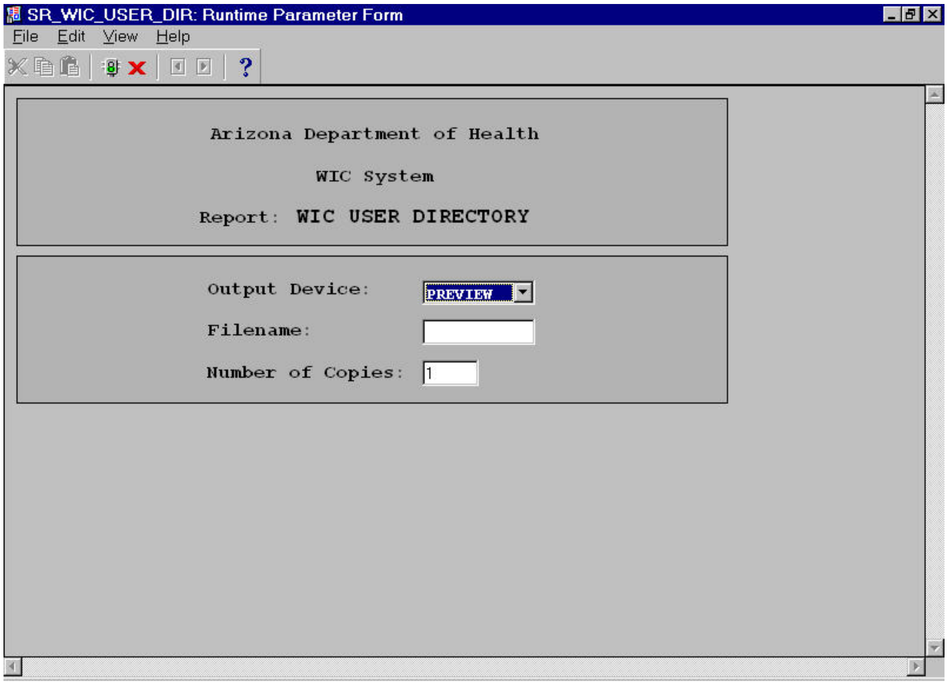
Producing a WIC User Directory Report

To Produce a WIC User Directory Report:

1. Click on Outputs from the menu bar.
2. Click on WIC User Directory as shown below:



The WIC User Directory Window is displayed:



Arizona Department of Health

WIC System

Report: WIC USER DIRECTORY

Output Device: PREVIEW

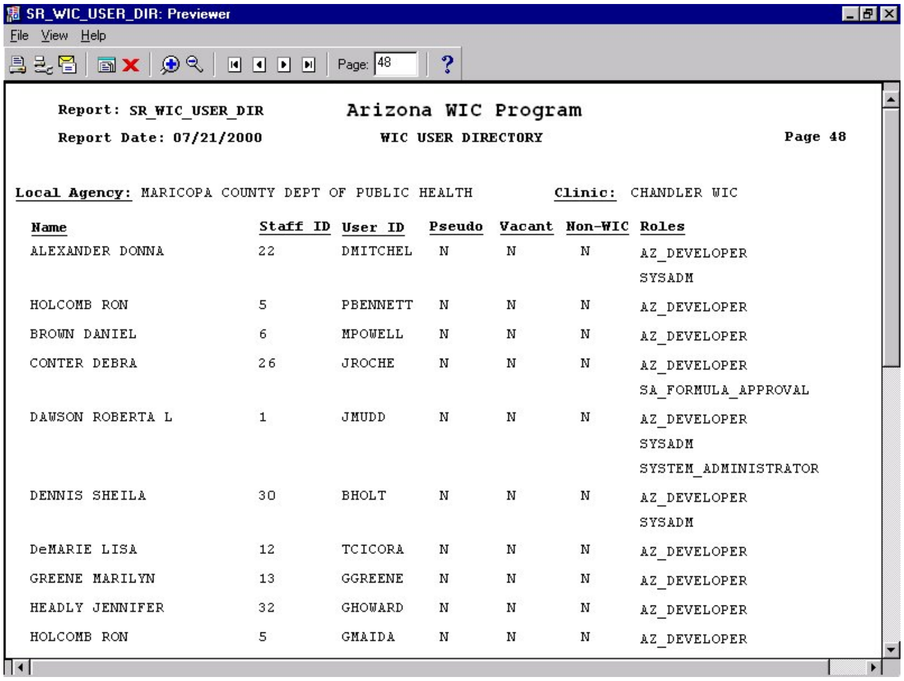
Filename:

Number of Copies: 1

Figure 45 - WIC User Directory Report

Produce a WIC User Directory Report

1. Click the down arrow in the Output Device field to activate the drop down box, then select which Output Device to send the WIC User Directory report to by double clicking on that device name.
2. TAB to the Filename field. Enter the filename to give to the report being generating.
3. TAB to the Number of Copies field. Select the number of report copies desired by typing in that number in this field.
4. Click the green light icon to bring up the preview screen shown below:



Report: SR_WIC_USER_DIR

Arizona WIC Program

Report Date: 07/21/2000

WIC USER DIRECTORY

Page 48

Local Agency: MARICOPA COUNTY DEPT OF PUBLIC HEALTH

Clinic: CHANDLER WIC

Name	Staff ID	User ID	Pseudo	Vacant	Non-WIC	Roles
ALEXANDER DONNA	22	DMITCHEL	N	N	N	AZ_DEVELOPER SYSADM
HOLCOMB RON	5	PBENNETT	N	N	N	AZ_DEVELOPER
BROWN DANIEL	6	MPOWELL	N	N	N	AZ_DEVELOPER
CONTER DEBRA	26	JROCHE	N	N	N	AZ_DEVELOPER SA_FORMULA_APPROVAL
DAWSON ROBERTA L	1	JMUDD	N	N	N	AZ_DEVELOPER SYSADM SYSTEM_ADMINISTRATOR
DENNIS SHEILA	30	BHOLT	N	N	N	AZ_DEVELOPER SYSADM
DeMARIE LISA	12	TCICORA	N	N	N	AZ_DEVELOPER
GREENE MARILYN	13	GGREENE	N	N	N	AZ_DEVELOPER
HEADLY JENNIFER	32	GHOWARD	N	N	N	AZ_DEVELOPER
HOLCOMB RON	5	GMAIDA	N	N	N	AZ_DEVELOPER

Figure 46 - WIC User Directory Report Sample

Sample WIC User Directory Report

5. Click the Previous, Next, First, Last, and Page icons at the top of the screen to move forward and backward through the report pages.
6. Click the Close icon to exit the preview screen. Click the New icon to view a new copy of the same preview screen.

Fields

Output Device - The User may select (from a drop down list) PREVIEW, SCREEN, PRINTER, HTML, RTF or PDF.
File Name - If file is selected (above), the directory and filename are entered.
Number of Copies - If printer is selected (above), the number of copies desired is entered.

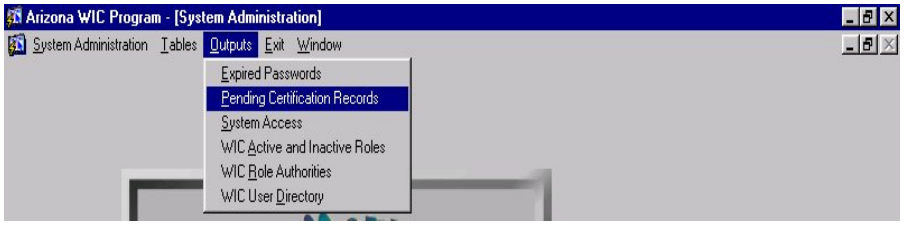
Calculations

None

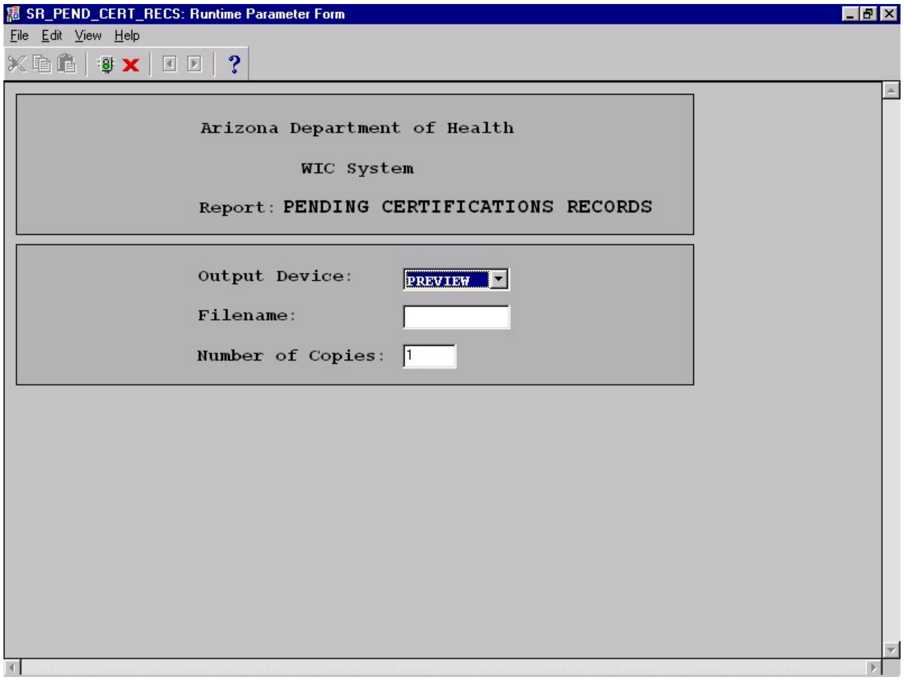
Producing a Pending Certification Records Report

To Produce a Pending Certifications Records Report:

1. Click on Outputs from the menu bar.
2. Click on Pending Certifications Records as shown below:



The Pending Certifications Records is displayed:



Arizona Department of Health

WIC System

Report: PENDING CERTIFICATIONS RECORDS

Output Device: PREVIEW

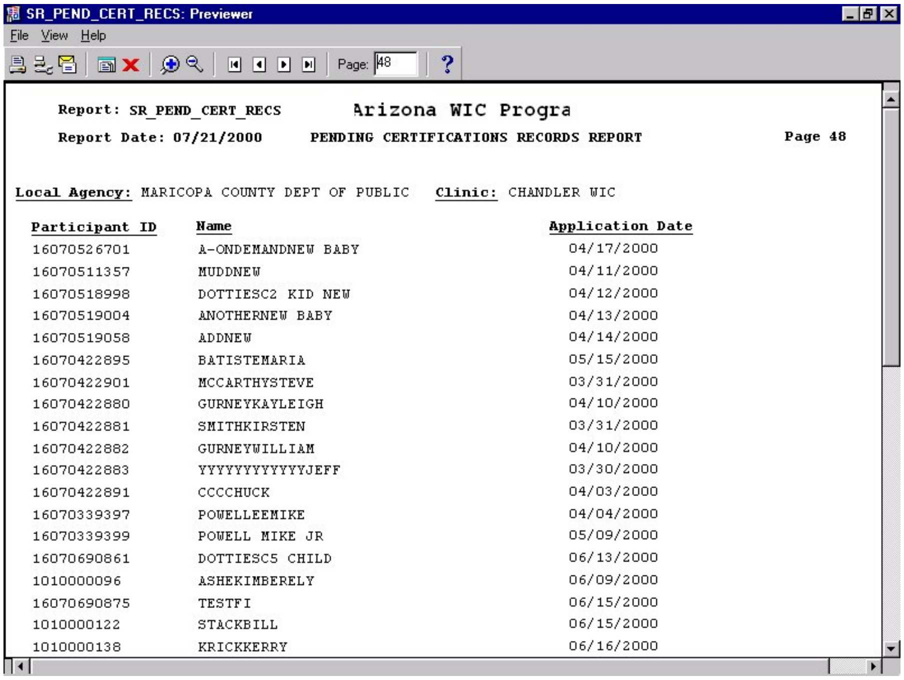
Filename:

Number of Copies: 1

Figure 47 - Pending Certifications Records

Produce a Pending Certifications Records Report

1. Click the down arrow in the Output Device field to activate the drop down box, then select which Output Device to send the Pending Certifications Records report to by double clicking on that device name.
2. TAB to the Filename field. Enter the filename to give to the report being generating.
3. TAB to the Number of Copies field. Select the number of report copies desired by typing in that number in this field.
4. Click the green light icon to bring up the preview screen shown below:



Report: SR_PEND_CERT_RECS Arizona WIC Progra

Report Date: 07/21/2000 PENDING CERTIFICATIONS RECORDS REPORT Page 48

Local Agency: MARICOPA COUNTY DEPT OF PUBLIC Clinic: CHANDLER WIC

Participant ID	Name	Application Date
16070526701	A-ONDEMANDNEW BABY	04/17/2000
16070511357	MUDDNEW	04/11/2000
16070518998	DOTTIESC2 KID NEW	04/12/2000
16070519004	ANOTHERNEW BABY	04/13/2000
16070519058	ADDNEW	04/14/2000
16070422895	BATISTEMARIA	05/15/2000
16070422901	MCCARTHYSTEVE	03/31/2000
16070422880	GURNEYKAYLEIGH	04/10/2000
16070422881	SMITHKIRSTEN	03/31/2000
16070422882	GURNEYWILLIAM	04/10/2000
16070422883	YYYYYYYYYYYYJEFF	03/30/2000
16070422891	CCCCHUCK	04/03/2000
16070339397	POWELLEEMIKE	04/04/2000
16070339399	POWELL MIKE JR	05/09/2000
16070690861	DOTTIESC5 CHILD	06/13/2000
1010000096	ASHEKIMBERELY	06/09/2000
16070690875	TESTFI	06/15/2000
1010000122	STACKBILL	06/15/2000
1010000138	KRICKKERRY	06/16/2000

Figure 48 - Pending Certifications Records

Sample Pending Certifications Records Report

5. Click the Previous, Next, First, Last, and Page icons at the top of the screen to move forward and backward through the report pages.
6. Click the Close icon to exit the preview screen. Click the New icon to view a new copy of the same preview screen.

Fields

Output Device - The User may select (from a drop down list) PREVIEW, SCREEN, PRINTER, HTML, RTF or PDF.
File Name - If file is selected (above), the directory and filename are entered.
Number of Copies - If printer is selected (above), the number of copies desired is entered.

Calculations

None

List of Figures